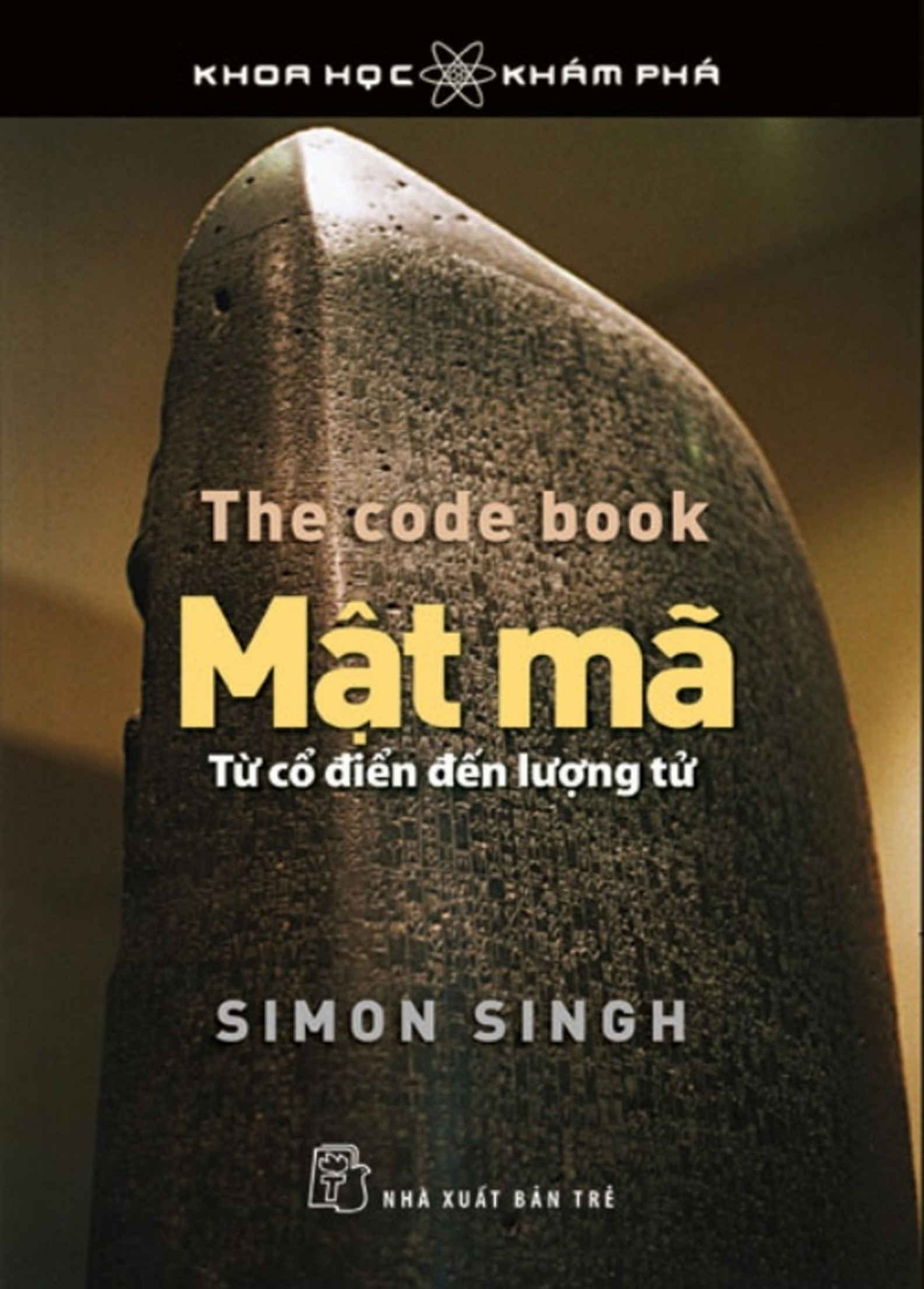
KHOA HỌC KHÁM PHÁ



The code book

Mật mã

Từ cổ điển đến lượng tử

SIMON SINGH

NHÀ XUẤT BẢN TRẺ

Mật mã

Từ cổ điển đến lượng tử

THE CODE BOOK. Tác giả Simon Singh
Copyright © 1999 By Simon Singh

BIỂU GHI BIÊN MỤC TRƯỚC XUẤT BẢN DO THƯ VIỆN KHTH TP.HCM THỰC HIỆN
General Sciences Library Cataloging-in-Publication Data

Singh, Simon
Mật mã - Từ cổ điển đến lượng tử / Simon Singh; ng. d. Phạm Văn Thiều, Phạm Thu Hằng. Tái bản lần thứ 4 - T.P. Hồ Chí Minh : Trẻ, 2014.
552 tr. ; 20 cm.
Nguyên bản: The Code Book
1. Mật mã. I. Phạm Văn Thiều d. II. Phạm Thu Hằng d. III. Ts. IV. Ts: The Code Book.

652.8 -- dc 22
S575

SIMON SINGH
PHẠM VĂN THIỀU - PHẠM THU HẰNG *dịch*

The code book

Mật mã

Từ cổ điển đến lượng tử

Tái bản lần thứ 4

NHÀ XUẤT BẢN TRẺ

Sự thôi thúc khám phá những bí mật đã ăn sâu vào bản chất của con người; ngay cả bộ não ít tò mò nhất cũng bị kích thích trước hứa hẹn sẽ được chia sẻ những thông tin bị che giấu từ người khác. Một số người đủ may mắn tìm được một công việc mà bản thân nó đã là nhằm khám phá những điều bí ẩn, còn hầu hết chúng ta buộc phải làm thăng hoa những thôi thúc đó bằng việc ngồi giải những trò chơi ô chữ do con người nghĩ ra để giải trí mà thôi. Những câu chuyện trinh thám hay trò chơi ô chữ nhằm làm thỏa mãn cho đại đa số, còn việc giải những bản mật mã thì có lẽ chỉ dành cho một số ít người theo đuổi.

John Chadwick
Giải mã Linear B

Mục lục

Mở đầu 9

1 Bản mật mã của Nữ hoàng Mary xứ Scotland 17
2 Le chiffre indéchiffrable..... 83
3 Cơ giới hóa việc giữ bí mật 157
4 Công phá Enigma..... 213
5 Rào cản ngôn ngữ 279
6 Alice và Bob ra công khai 349
7 Riêng tư tốt đẹp..... 421
8 Bước nhảy lượng tử vào tương lai 457

Phụ lục A..... 524
Phụ lục B..... 526
Phụ lục C..... 529
Phụ lục D 531
Phụ lục E..... 533
Phụ lục F 537
Phụ lục G 540
Phụ lục H 542
Phụ lục I..... 543
Phụ lục J..... 545
Các trang WEB tham khảo 549

Mở đầu

Trong hàng ngàn năm, vua chúa cũng như các tướng lĩnh đều dựa vào mạng lưới thông tin liên lạc hiệu quả để cai trị đất nước và chỉ huy quân đội của mình. Đồng thời, tất cả họ đều ý thức được những hậu quả của việc để lọt thông tin của mình vào tay đối phương, để lộ những bí mật quý giá cho các nước thù địch cũng như hậu quả của sự phản bội cung cấp thông tin sống còn cho các lực lượng đối kháng. Chính nỗi lo sợ bị kẻ thù xem trộm đã thúc đẩy sự ra đời và phát triển của mật mã: đó là những kỹ thuật nhằm che giấu, ngụy trang thông tin, khiến cho chỉ những người cần được nhận mới có thể đọc được.

Mong muốn giữ bí mật đã khiến các quốc gia thiết lập những cơ quan mật mã, có nhiệm vụ đảm bảo an toàn cho thông tin liên lạc bằng việc phát minh và sử dụng những mật mã tốt nhất có thể được. Trong khi đó, những người phá mã của đối phương cũng lại cố gắng để giải mã và đánh cắp những bí mật. Người giải mã là những nhà "giả kim thuật" về ngôn ngữ, một nhóm người bí ẩn chuyên tìm cách phỏng đoán những từ ngữ có nghĩa từ những ký hiệu vô nghĩa. Lịch sử của mật mã là câu chuyện về cuộc chiến kéo dài hàng thế kỷ giữa người lập mã và người giải mã, một cuộc chạy đua vũ khí trí tuệ đã có tác động rất to lớn đến tiến trình của lịch sử.

Khi viết cuốn *Mật mã* này, tôi có hai mục đích chính. Một là nhằm phác họa sự tiến hóa của mật mã. Từ tiến hóa dùng ở đây là hoàn toàn thích hợp vì sự phát triển của mật mã cũng có thể coi là một cuộc đấu tranh tiến hóa. Một mật mã luôn bị người phá mã tấn công. Khi người phá mã đã tìm ra một vũ khí mới để phát hiện điểm yếu của một mật mã thì mật mã đó không còn hữu dụng nữa. Khi đó, hoặc nó sẽ bị xóa sổ hoặc nó sẽ được cải tiến thành một loại mật mã mới, mạnh hơn. Đến lượt mình, mật mã mới này chỉ phát triển mạnh mẽ cho tới khi người phá mã lại xác định được điểm yếu của nó, và cứ tiếp tục mãi như vậy. Điều này cũng tương tự như tình huống đối mặt với một giống vi khuẩn gây bệnh chẳng hạn. Vi khuẩn sống, phát triển mạnh và tồn tại cho đến khi bác sĩ tìm ra chất kháng sinh làm lộ ra những điểm yếu của vi khuẩn và tiêu diệt nó. Vi khuẩn buộc phải tiến hóa và lừa lại kháng sinh, và nếu thành công thì chúng sẽ lại phát triển mạnh mẽ và tái xác lập trở lại. Vi khuẩn liên tục bị buộc phải tiến hóa để sống sót trước sự tấn công dữ dội của các loại kháng sinh mới.

Cuộc chiến liên miên giữa người lập mã và người phá mã đã thúc đẩy hàng loạt những đột phá khoa học đáng kể. Người lập mật mã đã liên tục cố gắng xây dựng những loại mã mạnh hơn bao giờ hết để bảo vệ thông tin, trong khi những người phá mã cũng lại kiên trì tìm ra những phương pháp mạnh hơn nữa để phá vỡ chúng. Trong những cố gắng nhằm phá vỡ và bảo vệ thông tin bí mật, cả hai phía đã phải huy động nhiều lĩnh vực chuyên môn và công nghệ khác nhau, từ toán học cho tới ngôn ngữ học, từ lý thuyết thông tin cho đến lý thuyết lượng tử. Đổi lại, những người lập mã và phá mã cũng đã làm giàu thêm cho những lĩnh

vực này và thành quả của họ đã đẩy nhanh tốc độ phát triển công nghệ, mà đáng kể nhất là trong lĩnh vực máy tính hiện đại.

Lịch sử được phân đoạn theo các loại mật mã. Chúng đã quyết định kết cục của các cuộc chiến và dẫn đến cái chết của nhiều vị vua chúa và nữ hoàng. Chính vì vậy mà tôi có thể sử dụng những câu chuyện về các âm mưu chính trị và những truyền thuyết về cuộc sống và cái chết để minh họa cho những bước ngoặt quan trọng trong quá trình tiến hóa của mật mã. Lịch sử mật mã phong phú một cách kỳ lạ khiến tôi buộc phải bỏ bớt đi rất nhiều câu chuyện hấp dẫn. Nếu bạn muốn tìm hiểu thêm những câu chuyện hoặc những người phá mã mà bạn ưa thích, tôi xin giới thiệu với các bạn một danh sách ở phần đọc thêm, nhằm giúp cho những ai muốn tìm hiểu vấn đề này một cách chi tiết hơn.

Sau khi đã bàn luận về sự tiến hóa của mật mã và những tác động của nó đến lịch sử, mục đích thứ hai của cuốn sách là nhằm chứng minh chủ đề này ngày nay còn trở nên hợp thời hơn bao giờ hết. Vì thông tin trở thành một loại hàng hóa có giá trị ngày một gia tăng và vì cuộc cách mạng về truyền thông làm thay đổi cả xã hội nên quá trình mã hóa thông tin sẽ đóng một vị trí ngày càng quan trọng trong đời sống hằng ngày của chúng ta. Ngày nay, các cuộc gọi điện thoại của chúng ta đều qua vệ tinh và các thư điện tử *(e-mail)* đi qua nhiều máy tính khác nhau, đồng thời cả hai loại giao tiếp này đều có thể bị nghe hoặc xem trộm khá dễ dàng, do vậy có nguy cơ làm tổn hại đến những bí mật riêng tư của chúng ta. Cũng tương tự như vậy, vì ngày càng có nhiều hoạt động kinh doanh được thực hiện qua Internet, nên sự bảo mật phải được thực hiện để bảo vệ cho các công ty và khách hàng của họ. Mã hóa là cách duy nhất để bảo vệ những bí mật riêng tư của

chúng ta và bảo đảm cho sự thành công của thị trường kỹ thuật số. Nghệ thuật truyền thông bí mật, hay nói cách khác là khoa học mật mã, sẽ cung cấp cả khóa lẫn chìa khóa của Thời đại Thông tin.

Tuy nhiên, nhu cầu ngày một tăng của xã hội đối với khoa học mật mã lại mâu thuẫn với yêu cầu tuân thủ luật pháp và bí mật quốc gia. Trong nhiều thập kỷ, cảnh sát và các cơ quan tình báo đã sử dụng biện pháp nghe trộm để thu thập chứng cứ chống lại bọn khủng bố và các tập đoàn tội phạm có tổ chức, song sự phát triển của những mã cực mạnh ngày nay đang đe dọa sẽ làm mất đi giá trị của việc nghe trộm đó. Khi chúng ta đang bước vào thế kỷ 21, những người theo chủ nghĩa tự do cá nhân đang gây sức ép cho việc sử dụng rộng rãi mã hóa để bảo vệ bí mật cá nhân. Đấu tranh cùng với họ là các doanh nhân, những người đòi hỏi phải mã hóa mạnh để bảo vệ bí mật giao dịch trong một thế giới phát triển chóng mặt của thương mại điện tử. Trong khi đó, các lực lượng luật pháp và trật tự lại vận động chính phủ hạn chế việc sử dụng mã hóa. Câu hỏi đặt ra là, chúng ta đánh giá cao việc nào hơn - bí mật riêng tư của chúng ta hay một lực lượng cảnh sát có hiệu quả? Hay cần phải có một sự thỏa hiệp?

Mặc dù mã hóa ngày nay có ảnh hưởng rất lớn đến các hoạt động dân sự, thì cũng cần lưu ý rằng mã hóa trong quân sự cũng vẫn là một lĩnh vực quan trọng. Người ta cho rằng Thế chiến thứ I là cuộc chiến tranh của các nhà hóa học, bởi vì khí mù tạt và clo lần đầu tiên được sử dụng, còn Thế chiến thứ II là chiến tranh của các nhà vật lý, vì bom nguyên tử đã được thả xuống. Tương tự, người ta cho rằng Thế chiến thứ III sẽ là cuộc chiến tranh của các nhà toán học bởi vì các nhà toán học sẽ điều khiển loại vũ khí vĩ đại tiếp theo của chiến tranh - đó là thông tin. Các nhà toán học

là những người chịu trách nhiệm phát triển các loại mã mà ngày nay đang được sử dụng để bảo vệ thông tin quân sự. Không có gì đáng ngạc nhiên khi chính các nhà toán học cũng lại là những người tiên phong trong cuộc chiến phá các loại mật mã đó.

Trong khi mô tả sự tiến hóa của mật mã và tác động của chúng đến lịch sử, tôi cũng tự cho phép mình đi lạc đề một chút. Chương 5 mô tả việc giải mã những văn bản cổ khác nhau, trong đó có bản *Linear B* và chữ viết tượng hình cổ Ai Cập. Về mặt kỹ thuật, mã hóa liên quan đến những cách truyền thông tin được thiết kế một cách cẩn trọng nhằm giữ bí mật đối với kẻ thù, trong khi đó thì những văn bản của các nền văn minh cổ đại lại hoàn toàn không có ý định viết ra để cho không ai có thể đọc được: đó chỉ đơn giản là do chúng ta đã mất khả năng diễn giải chúng mà thôi. Tuy nhiên, những kỹ năng cần thiết để khám phá ý nghĩa của những văn bản khảo cổ học cũng có quan hệ rất gần gũi với nghệ thuật giải mã. Ngay từ khi đọc cuốn *Giải mã Linear B* của John Chadwick mô tả quá trình đọc một văn bản cổ được tìm thấy ở Địa Trung hải, tôi đã bị cuốn hút bởi thành quả trí tuệ đáng kinh ngạc của những người đã giải mã được các văn bản của tổ tiên chúng ta, nhờ đó chúng ta mới biết được nền văn minh, tôn giáo và cuộc sống hằng ngày của họ.

Đối với những người ưa chính xác, tôi xin được thứ lỗi vì tựa đề của cuốn sách. Mật mã ở đây không chỉ nói riêng về mã từ *(code)*. Thuật ngữ "mã từ" hàm ý một dạng truyền thông bí mật rất cụ thể, một dạng mã đã lụi tàn qua nhiều thế kỷ sử dụng. Ở mã từ, một từ hay một cụm từ được thay thế bởi một từ, một con số hay một ký hiệu. Chẳng hạn, các điệp viên đều có bí danh, tức là các từ được sử dụng thay cho tên thật nhằm che giấu nhân dạng

của mình. Tương tự, cụm từ **Attack at dawn** (*Tấn công vào lúc bình minh*) có thể được thay thế bằng một từ mã là **Jupiter**, và từ này sẽ được gửi cho người chỉ huy trận đánh như một cách gây khó khăn cho đối phương. Nếu sở chỉ huy và viên tướng ngoài mặt trận đã thống nhất về mật mã trước đó, thì nghĩa của **Jupiter** là rất rõ ràng đối với người nhận, nhưng sẽ chẳng có nghĩa gì với đối phương khi chặn bắt được nó. Một cách tạo mã khác là mã thay thế chữ cái *(cipher),* đây là một kỹ thuật thực hiện ở mức độ cơ bản hơn, bằng cách thay thế các chữ cái chứ không phải là cả một từ hoặc cụm từ. Ví dụ, mỗi chữ cái trong một cụm từ có thể được thay thế bằng chữ cái tiếp theo trong bảng chữ cái, chẳng hạn như **A** được thay bằng **B, B** bằng **C**, v.v... Như vậy thì **Attack at dawn** sẽ trở thành **Buubdl bu ebxo**. Mã chữ cái đóng vai trò không thể thiếu trong khoa học mã hóa và vì vậy lẽ ra tên cuốn sách này phải là *Mã từ và mã chữ cái* mới phải. Tuy nhiên, tôi đã bỏ qua sự quá chi li đó cho ngắn gọn hơn.

Trước khi kết thúc phần giới thiệu, tôi phải lưu ý đến một vấn đề mà bất kỳ tác giả nào viết về vấn đề khoa học mật mã cũng gặp phải: đó là khoa học giữ bí mật, nhìn chung là một môn khoa học bí mật. Rất nhiều nhân vật trong cuốn sách này chưa bao giờ có được sự công nhận thành quả lúc sinh thời, vì những đóng góp đó không được công chúng biết đến rộng rãi, khi những phát minh của họ vẫn còn có giá trị quân sự hay ngoại giao. Trong khi tìm kiếm tư liệu để viết cuốn sách này, tôi đã được nói chuyện với nhiều chuyên gia thuộc Tổng hành dinh Thông tin Liên lạc của Chính phủ Anh (GCHQ), họ đã tiết lộ nhiều chi tiết về một nghiên cứu khác thường đã được thực hiện trong những năm 1970, chỉ vừa mới được loại khỏi danh mục bí mật. Chính nhờ

sự công bố này mà ba trong số những nhà khoa học mật mã vĩ đại nhất trên thế giới đã có được sự công nhận mà họ xứng đáng được hưởng. Tuy nhiên, sự tiết lộ này cũng chỉ có tác dụng nhắc nhở tôi rằng vẫn có những công trình lớn lao hơn đang được xúc tiến mà trong đó không một nhà văn khoa học nào kể cả tôi ý thức được. Các tổ chức như GCHQ và Cơ quan An ninh Quốc gia Mỹ vẫn không ngừng tiến hành những nghiên cứu bí mật về khoa học mật mã, có nghĩa là những khám phá của họ vẫn bí mật và những cá nhân làm ra chúng vẫn còn vô danh.

Mặc cho những vấn đề bí mật của chính phủ và những nghiên cứu còn đang được giữ kín, tôi vẫn dành chương cuối cùng trong cuốn sách này để dự đoán về tương lai của mật mã. Xét cho cùng, thì chương này là một cố gắng để xem xem liệu chúng ta có thể dự đoán ai sẽ chiến thắng trong cuộc đấu tranh tiến hóa giữa người tạo mã và người phá mã không. Liệu người lập mật mã có thiết kế được loại mã không thể phá được và thành công trong cuộc tìm kiếm cách giữ bí mật tuyệt đối của mình hay không? Hay những người phá mã sẽ chế tạo được một cỗ máy có thể giải mã bất kỳ thông tin nào? Hãy luôn nhớ rằng một số trong nhiều bộ não vĩ đại nhất hiện đang làm việc ở những phòng thí nghiệm bí mật, và họ nhận được những khoản tài trợ nghiên cứu khổng lồ, nên hiển nhiên là một vài tuyên bố của tôi trong chương cuối cũng có thể không chính xác. Chẳng hạn, tôi cho rằng các máy tính lượng tử - những máy tính có tiềm năng phá được tất cả loại mã đang dùng hiện nay - hiện vẫn đang ở trong một giai đoạn cực kỳ sơ khai, song cũng có thể có ai đó đã chế tạo được một cái rồi cũng nên. Những người duy nhất có thể chỉ ra sai lầm của tôi cũng lại chính là những người không được quyền tự do tiết lộ chúng.

1

Bản mật mã của Nữ hoàng Mary xứ Scotland

Buổi sáng thứ bảy, ngày 15 tháng Mười năm 1586, Nữ hoàng Mary bước vào phòng xử án chật ních người tại Lâu đài Fotheringhay. Những năm tù đày và sự hành hạ của căn bệnh phong thấp đã có những ảnh hưởng nhất định nhưng trông bà vẫn rất tôn quý, điềm tĩnh và uy nghi một cách không thể phủ nhận. Được dìu bởi người thầy thuốc của mình, bà đi qua các quan tòa, các vị chức sắc và những người chứng kiến, rồi tiến đến ngai vàng được đặt ở giữa căn phòng hẹp và dài. Mary đã tưởng chiếc ngai vàng đó như là một cử chỉ tôn kính đối với bà, nhưng bà đã lầm. Ngai vàng đó tượng trưng cho Nữ hoàng Elizabeth vắng mặt, kẻ thù và cũng là người xét xử Mary. Mary đã được người ta nhã nhặn dẫn đi khỏi ngai vàng về phía đối diện của căn phòng, tới chỗ ngồi của bị cáo, một chiếc ghế bọc nhung màu đỏ thẫm.

Nữ hoàng Mary xứ Scotland

Nữ hoàng Mary của Scotland đã bị mang ra xét xử vì mưu đồ tạo phản. Bà bị buộc tội đã âm mưu ám sát Nữ hoàng Elizabeth để cướp lấy vương miện nước Anh. Ngài Francis Walsingham, quan Thượng thư của triều đình Elizabeth, đã cho bắt những kẻ đồng phạm, lấy lời khai và đã hành quyết họ. Giờ đây ông ta dự định sẽ chứng minh Mary chính là chủ mưu và vì vậy bà cũng là kẻ phạm tội và cũng sẽ phải nhận án tử hình.

Walsingham biết rằng trước khi có thể xử tử Mary, ông phải thuyết phục được Nữ hoàng Elizabeth về sự phạm tội của bà ta. Mặc dù Elizabeth rất khinh ghét Mary, song bà ta cũng có một số lý do để lưỡng lự trong việc xử tội chết với Mary. Thứ nhất, Mary là một Nữ hoàng của xứ Scotland và sẽ có nhiều người đặt câu hỏi liệu một tòa án Anh có thẩm quyền để xử tử một người đứng đầu một quốc gia nước ngoài hay không. Thứ hai, xử tử Mary có thể sẽ tạo ra một tiền lệ xấu - nếu nhà nước cho phép giết một Nữ hoàng thì sau này có thể những kẻ nổi loạn sẽ ít e dè hơn khi giết một người khác, ấy là Elizabeth. Thứ ba, Elizabeth và Mary là chị em họ, nên mối ràng buộc huyết thống khiến Elizabeth còn khó khăn hơn trong việc ra lệnh xử tử Mary. Tóm lại, Elizabeth sẽ chuẩn y xử tử Mary chỉ khi Walsingham có

thể chứng minh được một cách chắc chắn rằng bà ta có tham gia trong âm mưu phản nghịch.

Những kẻ mưu phản là một nhóm những nhà quý tộc Anh trẻ tuổi theo Thiên chúa giáo, họ dự định lật đổ Elizabeth, người theo đạo Tin lành, và để Mary, cũng theo đạo Thiên chúa, lên thay. Điều rõ ràng đối với phiên tòa là Mary đúng là thủ lĩnh của nhóm mưu phản, nhưng lại chưa có bằng chứng là bà đã chấp thuận tham gia âm mưu này. Thực tế Mary là chủ mưu. Thách thức đối với Walsingham là phải chứng minh được mối liên hệ không thể chối cãi giữa Mary và những kẻ mưu phản.

Vào buổi sáng xét xử, Mary mặc một chiếc áo nhung đen sầu não, ngồi một mình trên ghế bị cáo. Trong những vụ án phản nghịch, bị cáo bị cấm không được có cố vấn và không được phép gọi nhân chứng. Tuy nhiên, cảnh ngộ của bà cũng không phải là vô vọng vì bà đã rất thận trọng đảm bảo để tất cả thư từ của bà với những kẻ mưu phản đều đã được viết bằng mật mã. Mật mã đã biến lời lẽ của bà thành dãy những ký hiệu vô nghĩa, và Mary tin rằng ngay cả khi Walsingham có bắt được những lá thư đó thì ông ta cũng chẳng hiểu được ý nghĩa của chúng. Nếu nội dung những lá thư này vẫn còn là điều bí ẩn thì chúng sẽ không thể được sử dụng làm bằng chứng chống lại bà được. Tuy nhiên, toàn bộ điều này còn tùy thuộc vào giả định rằng mật mã của bà không bị phá vỡ.

Thật không may cho Mary, Walsingham không chỉ đơn thuần là một quan Thượng thư, ông ta còn là một thám tử bậc thầy của nước Anh. Ông ta đã bắt được thư từ của Mary gửi cho những kẻ mưu phản và ông biết chính xác ai là người có khả năng giải mã

chúng. Thomas Phelippes là một chuyên gia hàng đầu quốc gia về việc giải mã và trong nhiều năm, ông đã giải mã được thư từ của những kẻ âm mưu chống lại Nữ hoàng Elizabeth, nhờ đó đã cung cấp những bằng chứng cần thiết để kết tội họ. Nếu ông ta có thể giải mã được những lá thư tội lỗi giữa Mary và đồng phạm thì cái chết của bà là không thể tránh khỏi. Nói cách khác, nếu mật mã của Mary đủ mạnh để che giấu được bí mật của mình thì bà sẽ có cơ may sống sót. Đây không phải là lần đầu tiên mạng sống của một người phụ thuộc vào sức mạnh của một mật mã.

Sự tiến hóa của thư từ bí mật

Một số bản chữ viết bí mật đầu tiên có từ thời Herodotus, mà theo nhà triết học và chính khách La mã Cicero, thì ông là "cha đẻ của lịch sử". Trong cuốn *Lịch sử*, Herodotus đã ghi lại theo niên đại những xung đột giữa Hy Lạp và Ba Tư ở thế kỷ thứ 5 trước công nguyên (CN), mà ông coi như là sự đối nghịch giữa tự do và nô lệ, giữa nền độc lập của nhà nước Hy Lạp và sự áp bức của người Ba Tư. Theo Herodotus, chính nghệ thuật viết thư bí mật đã cứu người Hy Lạp thoát khỏi sự thống trị của Xerxes, Vua của các vị Vua, tên bạo chúa của người Ba Tư.

Mối cừu hận kéo dài giữa Hy Lạp và Ba Tư đi đến hồi kết ngay sau khi Xerxes bắt đầu xây dựng một thành phố tại Perspolis, kinh đô mới của vương quốc ông ta. Những cống vật và quà tặng được gửi đến từ khắp mọi miền của vương quốc và những nước láng giềng, ngoại trừ Athens và Sparta. Quyết định báo thù cho sự lăng nhục này, Xerxes bắt đầu huy động lực lượng, và tuyên bố rằng "chúng ta sẽ mở rộng đế chế Ba Tư đến nơi mà biên giới của nó

là bầu trời riêng của Chúa, mặt trời sẽ không bao giờ chiếu sáng trên bất kỳ miền đất nào nằm ngoài biên giới của Ba Tư". Ông đã dành 5 năm sau đó để tập hợp một cách bí mật đội quân chiến đấu lớn nhất trong lịch sử, và sau đó, năm 480 trước CN, ông đã sẵn sàng tung ra một cuộc tấn công bất ngờ.

Tuy nhiên, việc xây dựng quân đội Ba Tư đã bị Demaratus, một người Hy Lạp bị trục xuất khỏi quê hương và đang sinh sống tại thành phố Susa của người Ba Tư, chứng kiến. Mặc dù bị trục xuất song ông vẫn trung thành với đất nước Hy Lạp, ông đã quyết định gửi thư báo cho người Sparta biết về kế hoạch tấn công của Xerxes. Khó khăn là ở chỗ làm thế nào để gửi thư đi mà không bị lính gác Ba Tư chặn bắt. Herodotus viết:

> Vì sự nguy hiểm bị phát hiện là rất lớn, nên chỉ có một cách mà theo ông có thể làm cho bức thư lọt qua được, đó là cạo lớp sáp bên ngoài hai thanh gỗ dầy, viết trên gỗ những gì Xerxes dự định làm, rồi phủ một lớp sáp ra ngoài. Bằng cách này, những thanh gỗ, trông rõ ràng là sạch trơn, sẽ không gặp phải khó khăn gì với bọn lính gác trên suốt đường đi. Khi thông báo đến nơi, không ai đoán ra điều bí mật, cho đến khi, theo tôi hiểu, con gái của Cleomenes là Gogo, vợ của Lenoidas, đã đoán được và nói với những người khác rằng nếu cạo lớp sáp đi, họ sẽ thấy những gì viết trên gỗ phía bên dưới. Và người ta đã làm như vậy; bức thông báo lộ ra, được đọc và sau đó được chuyển tới những người Hy Lạp khác.

Nhờ có sự báo trước, những người Hy Lạp đến lúc đó còn chưa phòng bị gì, giờ bắt đầu hối hả tự vũ trang. Lợi nhuận từ những mỏ bạc thuộc sở hữu của nhà nước, thường vẫn đem chia

cho dân chúng thì nay được chuyển hết cho quân đội để chế tạo hai trăm tàu chiến.

Xerxes đã đánh mất yếu tố sống còn là sự bất ngờ và, ngày 23 tháng Chín năm 480 trước CN, khi tàu chiến của Ba Tư tiến vào Vịnh Salamis gần Athens, thì người Hy Lạp đã sẵn sàng chống trả. Mặc dù Xerxes tin rằng ông ta đã bao vây hải quân của Hy Lạp, song người Hy Lạp đã khôn ngoan nhử cho tàu Ba Tư vào trong vịnh. Người Hy Lạp biết rằng tàu của họ, nhỏ hơn và ít hơn về số lượng, sẽ bị đập tan ngoài biển rộng, nhưng họ tin rằng bên trong ranh giới của vịnh, họ có thể thắng thế nhờ khôn ngoan hơn người Ba Tư. Vì gió đổi hướng, người Ba Tư nhận thấy họ đang bị đẩy vào vịnh và bị buộc phải chiến đấu theo những điều kiện của người Hy Lạp. Công chúa Ba Tư là Artemisia bị bao vây từ ba phía và cố gắng quay đầu ra biển nhưng lại đâm sầm vào một chiếc tàu của phía mình. Thế là cơn hoảng loạn bắt đầu. Càng lúc càng nhiều tàu Ba Tư đâm vào nhau và đúng lúc đó, người Hy Lạp tung ra một cuộc tấn công dữ dội, quyết liệt. Chỉ trong vòng một ngày, đội quân hùng hậu của Ba Tư đã bị hạ nhục.

Cách thức truyền tin bí mật của Demaratus chỉ dựa trên thủ thuật che giấu thư tín một cách đơn giản. Herodotus cũng ghi lại một trường hợp khác, trong đó việc che giấu đủ hiệu quả để đảm bảo cho việc chuyển tin được an toàn. Ông đã chép lại câu chuyện về Histaiaeus, người muốn bày tỏ sự ủng hộ Aristagoras xứ Miletus nổi dậy chống lại vua Ba Tư. Để chuyển những chỉ dẫn của mình đi một cách an toàn, Histaiaeus đã cạo tóc trên đầu người đưa tin, viết lên trên da đầu ông ta rồi chờ cho đến khi tóc mọc trở lại. Đây rõ ràng là một thời kỳ lịch sử còn chấp nhận sự thiếu khẩn trương ở một mức độ nhất định. Người đưa tin tất

nhiên không mang trên mình thứ gì dễ gây nghi ngờ, có thể đi lại mà không bị phiền toái gì. Khi đến nơi, ông ta lại cạo tóc của mình đi và chỉ cho người nhận những gì ghi trên đó.

Truyền tin bí mật dùng cách che giấu sự hiện hữu của thư tín được gọi là *kỹ thuật giấu thư (steganography* - có xuất xứ từ chữ *steganos* trong tiếng Hy Lạp, có nghĩa là "che đậy" và *graphein*, có nghĩa là "viết"). Trong hai ngàn năm kể từ thời Herodotus, nhiều dạng giấu thư đã được sử dụng trên khắp thế giới. Chẳng hạn, người Trung Quốc cổ đại đã viết thư trên một tấm lụa mỏng, sau đó được cuộn thành một quả cầu nhỏ xíu, rồi phủ sáp bên ngoài. Người đưa thư sẽ nuốt quả cầu sáp đó. Ở thế kỷ 16, nhà khoa học người Italia Giovanni Porta đã mô tả cách thức giấu thư trong một quả trứng đã luộc kỹ bằng cách chế tạo ra một loại mực từ hỗn hợp gồm 28g phèn và khoảng 0,57 lít dấm và sau đó sử dụng nó để viết trên vỏ trứng. Dung dịch thấm vào trong vỏ trứng và in bức thư lên trên bề mặt của lòng trắng trứng đã đặc lại, nó chỉ có thể đọc được sau khi bóc vỏ trứng. Giấu thư cũng bao gồm cả thủ pháp viết bằng mực không nhìn thấy được. Ngay từ thế kỷ 1 sau CN, Pliny the Elder đã giải thích cách thức chế tạo "mực" vô hình làm từ cây *thithymallus* như thế nào. Mặc dù vẫn còn trong suốt sau khi mực khô đi, song chỉ cần hơ nóng làm cháy mực là nó sẽ đổi sang màu nâu. Rất nhiều chất lỏng hữu cơ khác cũng có tác dụng tương tự vì chúng giàu carbon và vì vậy dễ cháy. Thực tế, khi hết loại mực vô hình được chế tạo công nghiệp, nhiều điệp viên hiện đại cũng đã biết ứng phó bằng cách dùng nước tiểu của chính mình!

Tuổi thọ của phương pháp giấu thư chứng tỏ rằng nó thực sự mang lại một chút an toàn, song lại có một điểm yếu rất cơ bản.

Nếu người đưa tin bị khám xét gắt gao và thư tín bị phát hiện thì nội dung thông tin sẽ bị lộ ngay lập tức. Việc chặn được thông tin sẽ tức thì làm nguy hại đến sự an toàn. Một người lính gác mẫn cán khám xét bất kỳ ai đi qua biên giới, cạo bất kỳ thanh phủ sáp ong nào, hơ nóng những mẩu giấy trắng trơn, bóc vỏ trứng luộc, cạo tóc trên đầu, v.v... thì nhất định sẽ có cơ hội phát hiện được thư tín bị che giấu.

Chính vì vậy, song song với việc phát triển kỹ thuật giấu thư, thì vẫn có sự tiến hóa của *khoa học mật mã* (*cryptography* - xuất xứ từ chữ *kryptos,* có nghĩa là "giấu kín"). Mục đích của mật mã không phải là che giấu sự tồn tại của thư tín mà là che giấu nội dung của nó, quá trình này được gọi là *mã hóa*. Để làm cho một bức thư trở nên không thể hiểu được, người ta mã hóa nó theo một thủ tục cụ thể đã được thỏa thuận trước giữa người gửi và người nhận. Như vậy, người nhận chỉ cần làm ngược lại thủ tục mã hóa là bức thư trở nên hiểu được. Lợi thế của việc mã hóa là nếu kẻ thù có chặn lấy được bức thư thì cũng không thể đọc được. Không biết thủ tục mã hóa, đối phương sẽ khó khăn, nếu không muốn nói là không thể, khôi phục trở lại bức thư gốc từ bức thư đã bị mã hóa.

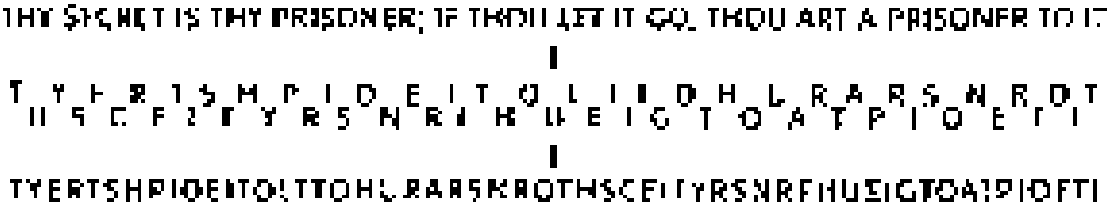
Tuy kỹ thuật giấu thư và khoa học mật mã là độc lập, song có thể sử dụng đồng thời việc mã hóa và giấu thư để đảm bảo an toàn tối đa. Chẳng hạn, vi ảnh là một dạng của kỹ thuật giấu thư đã được sử dụng phổ biến trong Thế chiến thứ II. Các điệp viên của Đức ở Mỹ Latin đã chụp thu nhỏ một trang giấy thành một chấm có đường kính nhỏ hơn 1mm, rồi sau đó giấu chấm cực nhỏ này trên dấu chấm câu của một bức thư bề ngoài vô thưởng vô phạt. Vi ảnh đầu tiên bị FBI phát hiện vào năm 1941, nhờ một

lời cảnh báo rằng người Mỹ cần phải tìm cho được một chấm nhỏ sáng mờ trên bề mặt của bức thư, đấy chính là dấu hiệu có giấu phim vi ảnh. Từ đó, người Mỹ đã đọc được nội dung của hầu hết các tấm vi ảnh bắt được trừ phi các điệp viên Đức thận trọng hơn đã tăng cường biện pháp an ninh bằng cách mã hóa thư của mình trước khi thu nhỏ lại. Trong những trường hợp có sự kết hợp giữa khoa học mật mã và kỹ thuật giấu thư như vậy, người Mỹ đôi khi cũng có thể chặn và phong tỏa liên lạc nhưng không thu được thêm thông tin mới nào về hoạt động gián điệp của Đức. Là một trong hai nhánh của thông tin liên lạc bí mật, song khoa học mật mã mạnh hơn là nhờ khả năng bảo vệ thông tin không cho rơi vào tay đối phương.

Bản thân mật mã có thể được chia ra làm hai nhánh, được gọi là *chuyển vị* và *thay thế*. Ở chuyển vị, các chữ cái trong thư được sắp xếp lại một cách đơn giản, tạo nên một phép đảo chữ một cách hiệu quả. Với những lá thư ngắn, chẳng hạn như chỉ gồm một từ duy nhất, thì phương pháp này không mấy an toàn, bởi vì với một số ít chữ cái thì chỉ có một số giới hạn cách sắp xếp. Chẳng hạn ba chữ cái có thể được sắp xếp lại theo 6 cách khác nhau, ví dụ: **cow, cwo, ocw, owc, wco, woc**. Tuy nhiên, khi số lượng chữ cái dần tăng lên thì số cách sắp xếp khả dĩ cũng tăng lên cực nhanh khiến cho không thể mò ngược trở lại thư gốc trừ phi đã biết trước chính xác quy trình mã hóa. Đối với câu: **For example, consider this short sentence** *(Ví dụ, hãy xét câu ngắn này)*, nó bao gồm 35 chữ cái và vì vậy có hơn 50.000.000.000.000.000.000.000.000.000.000 cách sắp xếp khác nhau. Nếu một người có thể kiểm tra một cách sắp xếp trong vòng 1 giây và tất cả mọi người trên Trái đất làm việc cả đêm lẫn ngày thì phải mất một khoảng thời

gian lớn gấp hàng ngàn lần tuổi của vũ trụ mới kiểm tra hết tất cả các cách sắp xếp đó.

Một sự chuyển vị ngẫu nhiên các chữ cái dường như mang lại một mức độ an toàn cao hơn, vì khi bắt được, đối phương cũng khó giải mã nổi, thậm chí ngay cả một câu ngắn. Nhưng nó cũng có một điểm yếu. Chuyển vị tạo ra một phép đảo chữ khó một cách đáng kinh ngạc, và nếu các chữ cái nhảy lộn xộn ngẫu nhiên không có lý do hay theo một chu kỳ nào cả thì việc giải mã nó là không thể thực hiện được cho cả người nhận đã định lẫn kẻ thù. Để việc chuyển vị có hiệu quả, việc sắp xếp các chữ cái cần phải theo một hệ thống không phức tạp lắm, được thống nhất trước giữa người nhận và người gửi, nhưng giữ bí mật đối với kẻ thù. Chẳng hạn, học sinh ở trường đôi khi gửi thư cho nhau sử dụng cách chuyển vị theo kiểu "hàng rào", trong đó, các chữ cái được viết luân phiên ở hàng trên và hàng dưới. Sau đó, câu tạo bởi các chữ cái ở hàng dưới được ghép vào sau câu tạo bởi các chữ cái ở hàng trên tạo thành một bức thư mã hóa hoàn chỉnh. Ví dụ:



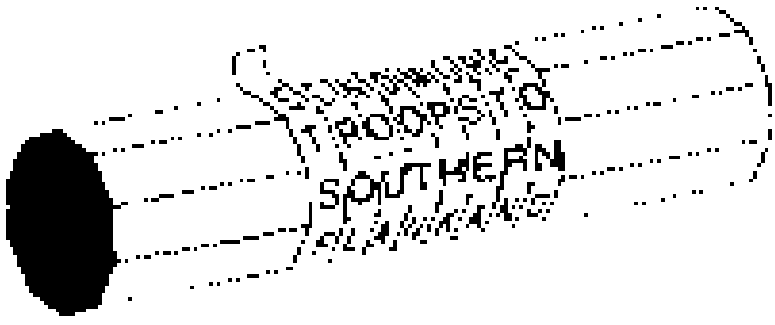
(Bí mật của mi là tù nhân của mi; nếu mi thả nó ra,
mi sẽ là tù nhân cho nó)

Người nhận có thể khôi phục lại bức thư bằng cách làm ngược lại quá trình trên một cách rất đơn giản. Có rất nhiều dạng chuyển vị có tính hệ thống, trong đó có cả mã hóa kiểu hàng rào ba dòng,

nghĩa là bức thư được viết trên ba dòng chữ chứ không phải hai dòng như ở trên. Ngoài ra, người ta cũng có thể đổi chỗ mỗi cặp hai chữ cái, chẳng hạn như hai chữ cái đầu tiên đổi chỗ cho nhau, chữ cái thứ ba và thứ tư đổi chỗ cho nhau, v.v...

Một dạng chuyển vị khác đã từng là một công cụ mã hóa sơ khai nhất trong quân đội, đó là *khúc gỗ bí mật* (scytale) của người Sparta, có từ thế kỷ thứ 5 trước CN. *Scytale* là một khúc gỗ có hình dạng và kích thước xác định được quấn quanh bằng một dải da như ở Hình 2. Người gửi viết thư theo chiều dài của khúc gỗ rồi sau đó bóc dải da ra, lúc này dải dây da chỉ mang trên nó một dãy những chữ cái vô nghĩa. Bức thư đã được mã hóa. Người mang tin sẽ chỉ mang dải dây da và, như một dạng của kỹ thuật giấu thư, người đó đôi khi có thể sử dụng nó như một cái thắt lưng với các chữ cái được giấu ở mặt sau. Để khôi phục lại bức thư, người nhận chỉ đơn giản quấn dây da đó quanh một cái *scytale* khác với kích thước giống như *scytale* của người gửi. Vào năm 404 trước CN, Lysander (người Sparta) gặp một người đưa thư, bị đánh đập và người bê bết máu, đó là người duy nhất trong số năm người còn sống sót trong cuộc hành trình đầy gian khổ trở về từ Ba Tư. Người đưa thư này đã đưa thắt lưng của mình cho Lysander, ông đã quấn nó quanh *scytale* của mình và biết được rằng Pharnabazus, vua xứ Ba Tư, đang có kế hoạch tấn công ông. Nhờ có *scytale*, Lysander đã kịp chuẩn bị và đẩy lùi được cuộc tấn công đó.

Ngoài chuyển vị, một cách mã hóa khác là thay thế. Một trong những mô tả đầu tiên về mã hóa sử dụng phương pháp thay thế xuất hiện trong *Kāma-Sūtra*, một bản viết tay ở thế kỷ 4 sau CN của nhà thông thái Bàlamôn tên là Vātsyāyana, dựa trên những



Hình 2. Khi được dỡ ra từ cây scytale của người gửi, dải da có vẻ như mang một dãy những chữ cái ngẫu nhiên: S, T, S, F,... Chỉ khi quấn lại dải da quanh một cây scytale khác, có đường kính tương ứng, bức thư mới được xuất hiện trở lại.

bản thảo có từ thế kỷ 4 trước CN. *Kāma-Sūtra* khuyên phụ nữ nên học sáu mươi tư nghệ thuật, như nấu ăn, may vá, massage, và làm nước hoa... Danh sách trên cũng bao gồm một số môn nghệ thuật ít rõ ràng hơn, như gọi hồn, chơi cờ, đóng sách và thợ mộc... Môn thứ bốn mươi lăm trong danh sách là *mlecchita-vikalpā,* nghệ thuật viết thư bí mật, nhằm giúp người phụ nữ che giấu những quan hệ bất chính của mình. Một trong những kỹ thuật được giới thiệu là tạo những cặp chữ cái trong bảng chữ cái một cách ngẫu nhiên, rồi sau đó mỗi chữ cái trong thư sẽ được thay thế bằng chữ cùng cặp với nó. Nếu chúng ta áp dụng nguyên tắc này cho bảng chữ cái La Mã, chúng ta có thể tạo các cặp chữ cái như sau:

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

Như vậy, thay vì viết **meet at midnight** *(gặp nhau lúc nửa đêm)*, người gửi thư sẽ viết **CUUZ VZ CGXSGIBZ**. Cách viết thư bí mật này được gọi là mã thay thế, vì mỗi chữ cái trong văn bản thường

được thay bằng một chữ cái khác, như vậy đây là một cách bổ sung cho mã chuyển vị. Trong mã chuyển vị mỗi chữ cái vẫn giữ nguyên dạng, chỉ thay đổi vị trí, còn trong mã thay thế thì các chữ cái chỉ thay đổi dạng (thành chữ cái khác), còn vị trí thì vẫn giữ nguyên.

Văn bản sử dụng mật mã thay thế đầu tiên cho mục đích quân sự xuất hiện trong cuốn *Chiến tranh xứ Gaul* của Julius Caesar. Caesar mô tả cách ông đã gửi thư cho Cicero, người bị vây hãm và đang ngấp nghé đầu hàng như thế nào. Đó là thay các chữ cái La Mã bằng các chữ cái Hy Lạp, khiến cho kẻ thù không thể hiểu nổi. Caesar đã mô tả việc gửi thư đầy kịch tính đó như sau:

> Người đưa thư được chỉ thị rằng, nếu anh ta không tiến tới gần được thì hãy phóng ngọn lao, với lá thư đã được buộc chặt vào sợi dây da, vào bên trong hào quanh trại. Lo sợ gặp nguy hiểm, gã người Gaul đã phóng ngọn lao như đã được chỉ dẫn. Tình cờ, ngọn giáo cắm sâu bên trong tháp nên trong hai ngày không ai nhìn thấy nó; đến ngày thứ ba một tên lính trông thấy, bèn lấy xuống và đưa nó cho Cicero. Ông ta đọc nó và sau đó đọc lại trước buổi duyệt quân, mang lại niềm phấn chấn lớn cho cả đội quân.

Caesar sử dụng mật mã thường xuyên đến nỗi Valerius Probus đã viết hẳn một chuyên luận về mật mã của ông nhưng không may là đã không còn giữ được đến ngày nay. Tuy nhiên, nhờ có cuốn *Cuộc đời của Caesar LVI* do Suetonius viết vào thế kỷ thứ 2 sau CN, chúng ta đã có được một sự mô tả chi tiết về một trong những dạng mật mã thay thế đã từng được Julius Caesar sử dụng. Ông đã thay thế một cách đơn giản từng chữ cái trong thư

bằng một chữ cái cách đó ba vị trí trong bảng chữ cái. Các nhà mật mã học thường tư duy thông qua *bảng chữ cái thường* (plain alphabet), tức là bảng chữ cái để viết nên bức thư gốc và *bảng chữ cái mật mã* (cipher alphabet), tức là những chữ cái được thay thế cho những chữ cái thường. Khi bảng chữ cái thường được đặt bên trên bảng chữ cái mật mã, như Hình 3, thì thấy rõ là bảng chữ cái mật mã đã bị dịch đi ba vị trí, và vì vậy dạng thay thế này được gọi là *mật mã dịch chuyển Caesar*, hay đơn giản là mã Caesar. Mã chữ cái là bất kỳ loại mật mã thay thế nào mà trong đó, mỗi chữ cái được thay bằng một chữ cái hoặc một ký hiệu khác.

Mặc dù Suetonius chỉ nói đến sự dịch chuyển ba vị trí của Caesar, song rõ ràng là bằng cách sử dụng sự dịch chuyển bất kỳ từ 1 đến 25 vị trí, ta có thể tạo ra 25 loại mật mã khác nhau. Thực ra, nếu chúng ta không hạn chế chỉ dịch bảng chữ cái, mà cho phép bảng chữ cái mật mã là sự sắp xếp lại bất kỳ nào của bảng chữ cái thường thì chúng ta có thể tạo ra một số lượng mật mã cực kỳ lớn. Có khoảng trên 400.000.000.000.000.000.000.000.000 cách sắp xếp như vậy và đó cũng chính là số loại mật mã khác nhau.

Mỗi loại mật mã có thể được xem xét thông qua phương pháp mã hóa tổng quát, được gọi là *thuật toán*, và một *chìa khóa mã*, xác định những chi tiết chính xác của một quá trình mã hóa cụ thể. Ở đây, thuật toán bao gồm cả việc thay thế một chữ cái trong bảng chữ cái thường bằng một chữ cái trong bảng chữ cái mật mã, và bảng chữ cái mật mã được phép bao gồm bất kỳ sự sắp xếp lại nào của bảng chữ cái thường. Chìa khóa mã xác định bảng chữ cái mật mã chính xác để sử dụng cho một thao tác mã hóa cụ thể. Mối quan hệ giữa thuật toán và chìa khóa mã được minh họa ở Hình 4.

Bảng chữ cái thường

a b c d e f g h i j k l m n o p q r s t u v w x y z

Bảng chữ cái mật mã

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Văn bản thường

v e n i, v i d i, v i c i

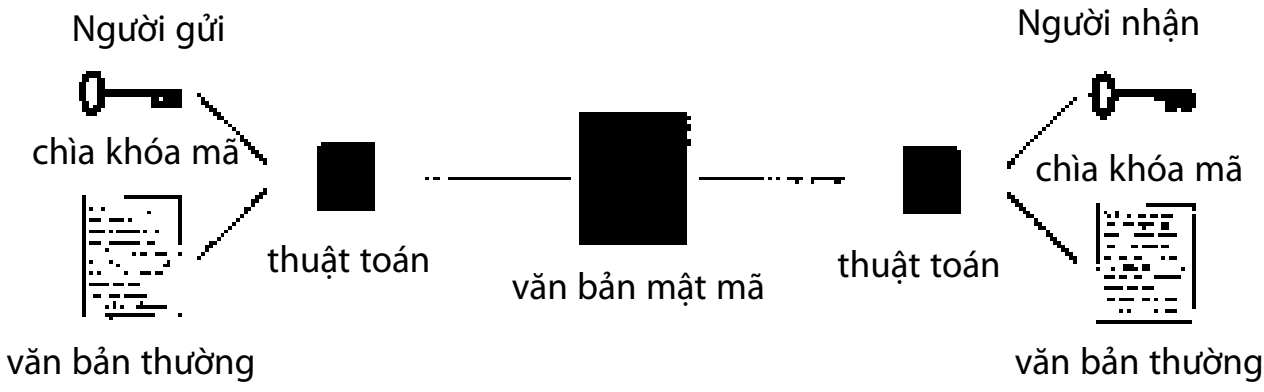
(đã tới, đã thấy, đã thắng)

Văn bản mật mã

Y H Q L, Y L G L, Y L F L

Hình 3. Mã Caesar áp dụng cho một bức thư ngắn. Mã Caesar dựa trên một bảng chữ cái mật mã, trong đó mỗi chữ cái dịch đi một số vị trí nhất định (trong trường hợp này là ba) so với bảng chữ cái thường. Quy ước trong mật mã học là viết bảng chữ cái thường bằng chữ thường còn bảng chữ cái mật mã viết bằng chữ in hoa. Tương tự, bức thư gốc, hay văn bản thường, được viết thường còn văn bản mật mã được viết bằng chữ in hoa.

Đối phương khi xem xét một bức thư mật mã chặn được có thể ngờ ngợ về thuật toán, song không biết chìa khóa mã chính xác. Ví dụ, họ có thể sẽ ngờ rằng mỗi chữ cái trong văn bản thường được thay thế bằng một chữ cái khác theo một bảng chữ cái mật mã nào đó, song họ không biết chắc chắn bảng chữ cái mật mã đã được sử dụng là như thế nào. Nếu bảng chữ cái mật mã cùng chìa khóa mã được giữ bí mật một cách nghiêm ngặt giữa người gửi và người nhận thì kẻ thù không thể giải mã được bức thư mà họ chặn bắt được. Ngược với thuật toán, chìa khóa mã có ý nghĩa là một nguyên tắc bền vững của mật mã học. Điều này đã được nhà ngôn ngữ học người Đức, Auguste Kerchhoffs phát biểu một cách dứt khoát vào năm 1883 trong cuốn *La cryptographie militare* (Mật mã quân sự): "Nguyên tắc Kerchhoffs: sự an toàn của một hệ thống



Hình 4. Để mã hóa một bức thư thường, người gửi chuyển nó qua một thuật toán mã hóa. Thuật toán là một hệ thống mã hóa chung, và cần phải được xác định một cách chính xác bằng việc lựa chọn một chìa khóa mã. Áp dụng cả chìa khóa mã và thuật toán cho một văn bản thường, ta sẽ tạo được một bức thư mật mã, hay văn bản mật mã. Văn bản mật mã có thể bị đối phương chặn bắt được khi nó đang trên đường chuyển đến cho người nhận, song họ không thể giải mã được bức thư. Tuy nhiên, người nhận, người biết cả chìa khóa mã và thuật toán đã được người gửi sử dụng, nên có thể chuyển văn bản mật mã trở lại thành văn bản thường.

mã hóa không phải phụ thuộc vào việc giữ bí mật thuật toán mã hóa. Độ an toàn chỉ phụ thuộc vào việc giữ bí mật chìa khóa mã".

Để giữ bí mật chìa khóa mã, một hệ thống mật mã an toàn phải có một số lượng chìa khóa mã tiềm tàng lớn. Chẳng hạn, nếu người gửi sử dụng mã dịch chuyển Caesar để mã hóa văn bản, thì sự mã hóa đó tương đối yếu vì chỉ có 25 chìa khóa mã tiềm tàng. Đứng ở góc độ kẻ thù, nếu họ bắt được thư và nghi ngờ thuật toán sử dụng là mã Caesar thì họ chỉ phải kiểm tra 25 khả năng. Tuy nhiên, nếu người gửi sử dụng thuật toán thay thế tổng quát hơn, cho phép bảng chữ cái mật mã là một sự sắp xếp bất kỳ của bảng chữ cái thường, thì sẽ có 400.000.000.000.000.000.000.000.000 chìa khóa mã tiềm tàng để lựa chọn. Một trong số đó được thể hiện ở Hình 5. Ở góc độ kẻ thù, nếu bức thư bị chặn được và thuật toán cũng đã được biết thì vẫn còn

một nhiệm vụ khủng khiếp nữa đó là kiểm tra tất cả các chìa khóa mã khả dĩ. Nếu một điệp viên đối phương mỗi giây đồng hồ có thể kiểm tra được một trong số 400.000.000.000.000.000.000.000.000 khả năng thì sẽ phải mất một khoảng thời gian lớn gấp 1 tỉ lần tuổi của vũ trụ mới kiểm tra được hết tất cả và giải mã được bức thư.

Nét đẹp của dạng mật mã này là nó rất dễ thực hiện, song lại cho độ an toàn cao. Người gửi dễ dàng xác định chìa khóa mã, đơn giản chỉ bằng cách nêu ra trật tự của 26 chữ cái trong bảng chữ cái mật mã được sắp xếp lại từ bảng chữ cái thường, và do vậy kẻ thù hoàn toàn không thể kiểm tra được tất cả các chìa khóa mã khả dĩ bằng cái gọi là sự tấn công hùng hục được. Sự đơn giản của chìa khóa mã là rất quan trọng, vì người gửi và người nhận phải cho nhau biết về chìa khóa mã, và chìa khóa mã càng đơn giản thì càng ít có khả năng hiểu nhầm.

Bảng chữ cái thường
a b c d e f g h i j k l m n o p q r s t u v w x y z
Bảng chữ cái mật mã
J L P A W I Q B C T R Z Y D S K E G F X H U O N

Văn bản thường	e t	t u ,	b r u t e ?
Văn bản mật mã	W X	X H ,	L G H X W ?

Hình 5. Một ví dụ về thuật toán thay thế tổng quát, trong đó mỗi chữ cái trong văn bản thường được thay thế bằng một chữ cái khác theo một chìa khóa mã. Chìa khóa mã được xác định bởi bảng chữ cái mật mã, có thể là một sự sắp xếp lại bất kỳ nào của bảng chữ cái thường.

Trong thực tế, một chìa khóa mã đơn giản hơn vẫn có thể có được nếu người gửi sẵn sàng chấp nhận giảm bớt đi đôi chút số

chìa khóa mã khả dĩ. Thay vì sắp xếp lại một cách ngẫu nhiên bảng chữ cái thường để tạo ra bảng chữ cái mật mã, người gửi có thể lựa chọn một *từ khóa mã* hoặc *cụm từ khóa mã*. Chẳng hạn, để sử dụng **JULIUS CAESAR** làm một cụm từ khóa mã, hãy bắt đầu bằng việc bỏ đi các dấu cách và các chữ cái trùng nhau (**JULISCAER**), sau đó sử dụng nó làm thành các chữ cái đầu trong bảng chữ cái mật mã. Phần còn lại của bảng chữ cái mật mã chỉ gồm các chữ cái còn lại trong bảng chữ cái thường, theo đúng trật tự của chúng, bắt đầu từ chữ cái tiếp ngay sau chữ cái cuối cùng trong cụm từ khóa mã. Do đó, bảng chữ cái mật mã bây giờ có dạng sau:

Bảng chữ cái thường
a b c d e f g h i j k l m n o p q r s t u v w x y z
Bảng chữ cái mật mã
J U L I S C A E R T V W X Y Z B D F G H K M N O P Q

Lợi thế của việc thiết lập một bảng chữ cái mật mã theo phương pháp này là từ khóa mã hay cụm từ khóa mã rất dễ nhớ và bảng chữ cái mật mã cũng vậy. Điều này rất quan trọng vì nếu người gửi phải ghi bảng chữ cái lên một mẩu giấy thì kẻ thù có thể bắt được mẩu giấy đó, khám phá ra chìa khóa mã và nhờ nó đọc được bất kỳ thông tin nào. Tuy nhiên, nếu chìa khóa mã được ghi trong đầu thì sẽ ít khả năng bị rơi vào tay kẻ thù. Tất nhiên, số lượng các bảng chữ cái mật mã được tạo bởi cụm từ khóa mã là ít hơn số lượng các bảng chữ cái mật mã được tạo ra mà không hề có một sự hạn chế nào, song vẫn còn khá lớn và kẻ thù không thể thử tất cả các cụm từ khóa mã để giải mã bức thư được.

Chính tính đơn giản và vững chắc khó phá vỡ này của mã thay thế đã khiến cho nó có vị trí thống trị trong nghệ thuật thư tín

bí mật trong suốt thiên niên kỷ thứ nhất sau CN. Những người tạo mật mã có nhiệm vụ phát triển một hệ thống bảo đảm cho thông tin liên lạc được an toàn, do vậy họ không có nhu cầu phải phát triển tiếp, nếu không thấy cần thiết. Gánh nặng bây giờ đè lên vai những người phá mã, họ có nhiệm vụ phải phá cho được mã thay thế. Liệu có cách nào cho đối phương đọc được một bức thư mã hóa như thế hay không? Rất nhiều học giả cổ đại cho rằng mã thay thế là không thể phá nổi, bởi một số lượng khổng lồ các chìa khóa mã tiềm năng, và trong nhiều thế kỷ, điều này dường như là sự thật. Tuy nhiên, các nhà giải mã cuối cùng cũng đã tìm ra một phương pháp nhanh gọn cho quá trình tìm kiếm tất cả các chìa khóa mã khả dĩ một cách triệt để. Thay vì phải mất hàng tỉ năm mới phá nổi một mật mã thì với phương pháp này chỉ tính bằng phút. Khám phá này được thực hiện ở phương Đông và đòi hỏi một sự kết hợp tuyệt diệu những đóng góp của ngôn ngữ học, thống kê học và tôn giáo.

Các nhà phân tích mã ả Rập

Ở tuổi 40, Muhammad bắt đầu thường xuyên lui tới một cái hang nằm cô độc trên núi Hira, ngay bên ngoài thánh địa Mecca. Đó là một nơi ẩn cư, một chỗ để cầu nguyện, suy tư và chiêm nghiệm. Vào khoảng năm 610 sau CN, trong một lần đang chìm đắm trong suy tư, ông đã được tổng lãnh thiên thần Gabriel viếng thăm và tuyên bố Muhammad được phong là nhà tiên tri của Chúa. Đây là sự kiện đầu tiên trong hàng loạt những mặc khải tiếp diễn sau này cho đến khi Muhammad qua đời vào khoảng 20 năm sau đó. Những mặc khải này được nhiều người ghi chép lại trong suốt

cuộc đời của Nhà tiên tri, song rất rời rạc, và được để lại cho Abū Bakr, vị vua Hồi giáo *(caliph)* đầu tiên, người đã tập hợp chúng lại thành một văn bản. Công việc này tiếp tục được thực hiện bởi Umar, vị vua thứ hai, và cô con gái Hafsa của ông ta và cuối cùng được Uthmān, vị vua thứ ba, hoàn tất. Mỗi một mặc khải này đều đã trở thành một chương trong 114 chương của Kinh Koran.

Các vị vua cầm quyền đều có trách nhiệm thực hiện công việc của Nhà tiên tri, gìn giữ những lời giáo huấn của ông và truyền bá lời ông nói. Trong khoảng thời gian từ lúc Abū Bakr lên làm vua năm 632 cho đến khi vị vua thứ tư là Ali qua đời vào năm 661, đạo Hồi đã được truyền bá rộng rãi tới mức một nửa thế giới nằm dưới sự cai trị của người Hồi giáo. Vào năm 750, sau một thế kỷ củng cố vững chắc, sự khởi đầu của triều đại Abbasid đã báo hiệu một thời đại hoàng kim của nền văn minh Hồi giáo. Nghệ thuật và khoa học cùng song hành phát triển rực rỡ. Các nghệ nhân Hồi giáo đã để lại cho chúng ta những bức tranh tuyệt vời, những bức chạm khắc lộng lẫy, và những tấm lụa tinh xảo nhất trong lịch sử, còn di sản của các nhà khoa học Hồi giáo cũng không kém phần vĩ đại, bằng chứng là số lượng các từ Ả Rập trong hệ thống thuật ngữ của khoa học hiện đại là rất lớn, chẳng hạn như *algebra* (đại số học), *alkaline* (tính kiềm) và *zenith* (thiên đỉnh)...

Sự giàu có của nền văn hóa Hồi giáo phần lớn là nhờ một xã hội hòa bình và thịnh vượng. Các vị vua thuộc triều đại Abbasid ít quan tâm tới việc đi chinh phục như những vị vua trước mà tập trung vào việc xây dựng một xã hội có tổ chức và hưng thịnh. Thuế khóa thấp hơn đã khuyến khích việc kinh doanh, khiến cho thương mại và công nghiệp phát triển mạnh mẽ, trong khi

đó pháp luật nghiêm khắc đã làm giảm nạn tham nhũng và bảo vệ được công dân. Tất cả những điều này đều dựa trên một hệ thống cai trị hiệu quả và đến lượt mình, những người cai trị lại dựa trên một hệ thống thông tin liên lạc an toàn đạt được nhờ sử dụng mật mã. Ngoài việc mã hóa những vấn đề nhạy cảm của đất nước, những tài liệu còn lại tới nay cũng cho biết rằng quan lại cũng đã giữ bí mật được các số liệu về thuế, điều này cho thấy việc sử dụng mật mã thời đó là rộng khắp và phổ biến. Một bằng chứng nữa có được là từ những cuốn sách hướng dẫn việc cai trị, chẳng hạn như cuốn *Adab al-Kutāb* (Sách hướng dẫn nghề thư ký) ở thế kỷ thứ 10, trong đó cũng có những phần nói về kỹ thuật mã hóa.

Những người cai trị thường sử dụng bảng chữ cái mật mã đơn giản chỉ là một sự sắp xếp lại bảng chữ cái thường như đã mô tả trước đây, song họ cũng sử dụng những bảng chữ cái mật mã có chứa một số loại ký hiệu khác. Chẳng hạn, **a** trong bảng chữ cái thường có thể được thay thế bằng # trong bảng chữ cái mật mã, **b** thay bằng +, v.v... *Mã thay thế dùng một bảng chữ cái* (monoalphabetic substitution cipher) là tên chung chỉ các loại mật mã thay thế mà trong đó bảng chữ cái mật mã bao gồm các chữ cái, hoặc các ký hiệu hoặc kết hợp cả hai. Tất cả các loại mật mã thay thế mà chúng ta đã gặp đến nay đều thuộc nhóm chung này.

Nếu như người Ả Rập quá quen thuộc với việc sử dụng mã thay thế dùng một bảng chữ cái, thì họ lại không để lại ấn tượng đáng kể nào trong lịch sử tạo mật mã. Tuy nhiên, ngoài việc sử dụng mật mã, các học giả Ả Rập cũng đã có khả năng phá được mật mã. Và thực tế thì họ đã phát minh ra *phép phân tích mã* (cryptanalysis), môn khoa học có nhiệm vụ giải mã một bức thư

mà không biết chìa khóa mã. Trong khi các nhà tạo mã phát triển những phương pháp mới để viết các thư tín bí mật, thì những người phân tích mã lại cố gắng tìm ra những điểm yếu trong các phương pháp này hòng đột phá vào những thư tín mật. Các nhà phân tích mã Ả Rập đã thành công trong việc tìm ra một phương pháp phá được mã thay thế dùng một bảng chữ cái, một loại mật mã đã từng được mệnh danh là không thể phá nổi trong nhiều thế kỷ.

Khoa học phân tích mã không thể được phát minh nếu như xã hội chưa đạt tới một trình độ học thuật phức tạp nhất định ở một số lĩnh vực như toán học, thống kê học và ngôn ngữ học. Nền văn minh Hồi giáo đã tạo ra cái nôi lý tưởng cho khoa học phân tích mã ra đời, vì Hồi giáo đòi hỏi công lý trong tất cả mọi lĩnh vực hoạt động của con người, và để đạt được điều đó thì đòi hỏi phải có kiến thức hay *ilm*. Mọi người Hồi giáo đều được phép theo đuổi tri thức dưới mọi hình thức và những thành công về kinh tế của triều đại Abbasid chứng tỏ rằng các học giả đã có thời gian, tiền bạc và phương tiện vật chất cần thiết để thực hiện phận sự của mình. Họ đã nỗ lực tiếp thu kiến thức từ những nền văn minh đi trước bằng cách tiếp nhận các tài liệu của người Ai Cập, Babylon, Ấn, Trung Hoa, Ba Tư, Syri, Armenia, Hebre và La Mã và dịch chúng ra tiếng Ả Rập. Năm 815, vua al-Ma'mūn đã cho xây dựng ở Baghdad một Bait al-Hikmah (có nghĩa là "Ngôi nhà thông thái"), thực chất là một thư viện và trung tâm dịch thuật.

Đồng thời với việc tiếp thu kiến thức, nền văn minh Hồi giáo cũng còn góp phần truyền bá kiến thức, bởi vì họ đã lấy được nghệ thuật làm giấy của người Trung Hoa. Sản xuất ra giấy đã làm xuất hiện nghề *warraqīn*, tức là "nghề cạo giấy", thực chất

đó là "những máy-photocopy-người" chuyên có nhiệm vụ sao chép lại bản thảo và đã đáp ứng được cho ngành công nghiệp xuất bản đang bùng phát lúc bấy giờ. Vào thời điểm nở rộ, hàng chục ngàn cuốn sách được xuất bản mỗi năm và chỉ riêng ở một vùng ngoại ô của thành Baghdad cũng đã có trên một trăm hiệu sách. Cùng với những cuốn sách cổ điển như *Ngàn lẻ một đêm*; những hiệu sách này cũng bán cả sách giáo khoa về mọi chủ đề có thể tưởng tượng ra được và đã giúp duy trì một xã hội học thức nhất trên thế giới.

Ngoài sự hiểu biết sâu rộng hơn về các môn học "trần tục" ra, sự phát minh ra khoa học phân tích mã cũng còn phụ thuộc vào sự phát triển của học vấn tôn giáo. Nhiều trường thần học lớn được dựng lên ở Basra, Kufa và Baghdad, đây là nơi để các nhà thần học tiến hành nghiên cứu những mặc khải của Muhammad có trong kinh Koran. Họ rất quan tâm đến việc xác lập niên đại của những mặc khải đó, bằng cách đếm tần suất xuất hiện của các từ trong mỗi mặc khải. Lý thuyết của họ dựa trên nhận xét rằng, có những từ tương đối mới xuất hiện, do vậy nếu một mặc khải nào có chứa nhiều từ mới hơn này thì đó chính là những mặc khải có niên đại sau. Các nhà thần học cũng nghiên cứu cả cuốn *Hadīth*, trong đó ghi chép những lời nói hằng ngày của Nhà tiên tri. Họ cố gắng chứng minh rằng mỗi phát ngôn đó đều thực sự thuộc về Muhammad. Điều này được thực hiện bằng cách nghiên cứu nguồn gốc của các từ và cấu trúc câu, để kiểm tra xem mỗi bản chép riêng biệt có phù hợp với kiểu cách ngôn ngữ của Nhà tiên tri hay không.

Điều quan trọng là các học giả tôn giáo không chỉ dừng sự nghiên cứu của họ ở cấp độ các từ. Họ còn phân tích cả từng

chữ cái một và đặc biệt là họ đã khám phá ra rằng một số chữ cái thông dụng hơn những chữ cái khác. Chữ cái **a** và **l** là thông dụng nhất trong tiếng Ả Rập, một phần là vì mạo từ xác định **al-**, trong khi chữ cái **j** lại xuất hiện với tần suất khoảng 1/10. Sự quan sát bề ngoài có vẻ là vô hại này đã dẫn đến đột phá vĩ đại đầu tiên trong khoa học phân tích mã.

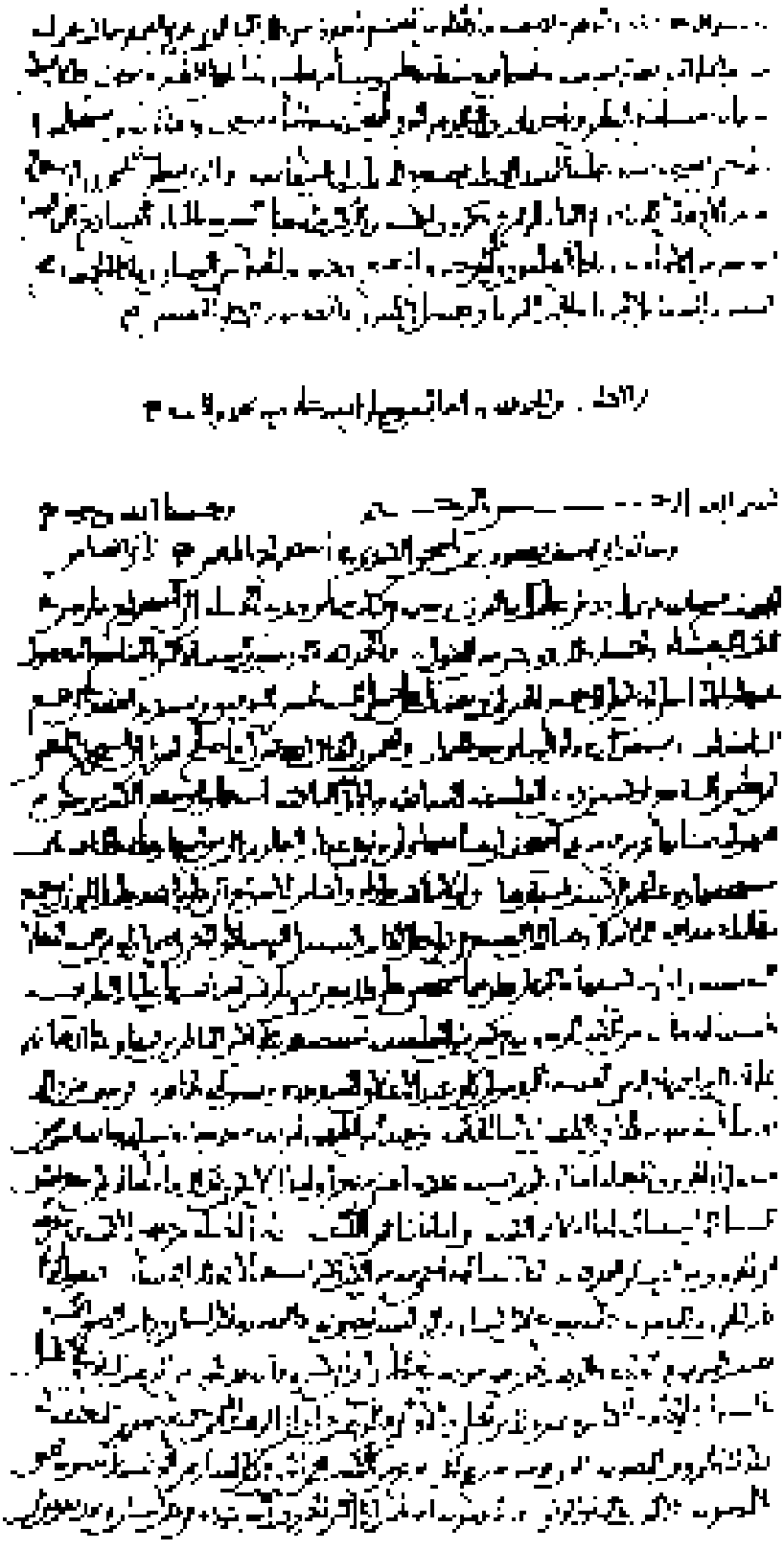
Mặc dù chúng ta không biết ai là người đầu tiên phát hiện ra sự biến thiên trong tần suất xuất hiện của các chữ cái có thể được khai thác để phá mã, song sự mô tả được biết đến sớm nhất về kỹ thuật này là bởi nhà khoa học thế kỷ thứ 9 Abū Yūsūf Yaʾqūb ibn Is-hāq ibn as-Sabbāh ibn ʿomrān ibn Ismaīl al-Kindī. Được biết đến như là "nhà hiền triết của Ả Rập", al-Kindī là tác giả của 290 cuốn sách về y học, thiên văn học, toán học, ngôn ngữ học và âm nhạc. Chuyên luận vĩ đại nhất của ông, chỉ mới được tái khám phá vào năm 1987 tại Cục lưu trữ Sulaimaniyyah Ottoman ở Istanbul, có nhan đề *Khảo cứu về giải mã các thư tín mật mã;* trang đầu tiên của cuốn sách này được in lại trên Hình 6. Tuy cuốn sách có những thảo luận chi tiết về thống kê học, ngữ âm và cú pháp Ả Rập, nhưng hệ thống phân tích mã có tính cách mạng của al-Kindī chỉ được gói gọn trong hai đoạn ngắn như sau:

> Một cách để giải một bức thư được mã hóa, nếu chúng ta biết ngôn ngữ của nó, là tìm một văn bản thường khác, cùng loại ngôn ngữ dài đủ một trang hoặc tương đương, rồi đếm số lần xuất hiện của từng chữ cái. Chúng ta gọi chữ cái xuất hiện nhiều nhất là "thứ nhất", chữ cái xuất hiện nhiều tiếp theo là "thứ hai", sau đó là "thứ ba", v.v... cho đến khi chúng ta đếm đến hết các chữ cái khác trong văn bản thường này.

> Sau đó, nhìn vào văn bản mật mã mà chúng ta muốn giải mã và cũng tiến hành phân loại các ký hiệu trong đó. Chúng ta tìm ký hiệu xuất hiện nhiều nhất và đổi nó thành chữ cái "thứ nhất" ở văn bản thường, ký hiệu xuất hiện nhiều tiếp theo đổi thành chữ cái "thứ hai", v.v... cho đến khi chúng ta thay hết các chữ cái trong bản mật mã mà chúng ta muốn giải mã.

Sự trình bày của al-Kindī dễ giải thích hơn với bảng chữ cái tiếng Anh. Trước hết, cần thiết phải nghiên cứu một đoạn văn bản dài bằng tiếng Anh thường, có thể là một vài đoạn, để thiết lập tần suất của mỗi chữ cái trong bảng chữ cái. Trong tiếng Anh, **e** là chữ cái thông dụng nhất, tiếp theo là **t, a** như trình bày ở Bảng 1. Sau đó, kiểm tra văn bản mật mã cần giải mã và tìm tần suất của mỗi chữ cái trong đó. Nếu chữ cái thông dụng nhất trong văn bản mật mã, chẳng hạn là **J**, thì gần như chắc chắn là nó đã thay thế cho chữ cái **e**. Và nếu chữ cái thông dụng thứ hai trong văn bản mật mã là **P**, thì nó có thể thay thế cho **t**, và cứ tiếp tục như vậy. Kỹ thuật của al-Kindī, được gọi là *phân tích tần suất*, cho thấy không nhất thiết phải kiểm tra từng chìa khóa mã trong số hàng tỉ chìa khóa mã khả dĩ. Thay vì, ta có thể tìm ra nội dung của thông tin được mã hóa một cách đơn giản bằng cách phân tích tần suất của các ký tự trong văn bản đã mã hóa.

Tuy nhiên, không thể áp dụng phương pháp của al-Kindī để phân tích mã một cách vô điều kiện được, vì danh sách tần suất chuẩn ở Bảng 1 chỉ là tính trung bình, và nó không tương ứng một cách chính xác với tần suất ở mọi văn bản. Chẳng hạn, một đoạn văn ngắn sau nói về ảnh hưởng của khí quyển đối với sự di chuyển của ngựa vằn châu Phi sẽ không tuân thủ theo sự phân



Hình 6. Trang đầu tiên trong cuốn *Về giải mã các thư tín bí mật* của al-Kindī, trong đó có đoạn mô tả được cho là cổ nhất về phép phân tích mã bằng tần suất.

tích tần suất một cách giản đơn: "Các vùng ôzôn từ Zanzibar đến Zambia và Zaire làm cho ngựa vằn chạy theo những con đường zic-zắc rất kỳ cục". Nhìn chung, những văn bản ngắn chắc chắn sẽ sai lệch đáng kể so với các tần suất chuẩn và nếu có ít hơn một trăm chữ cái thì việc giải mã sẽ rất khó khăn. Trái lại, những văn bản dài hơn thì chắc chắn sẽ tuân theo tần suất chuẩn hơn, mặc dù không phải lúc nào cũng như vậy. Năm 1969, một tác giả người Pháp tên là Georges Perec đã viết cuốn *La Disparition* (Sự biến mất), một cuốn tiểu thuyết dày 200 trang mà trong đó không hề có từ nào chứa chữ cái **e**. Đáng kể hơn nữa là tiểu thuyết gia và nhà phê bình người Anh Gilbert Adair đã thành công trong việc dịch cuốn *La Disparition* sang tiếng Anh mà vẫn tuân thủ việc chừa ra chữ cái **e** của Perec. Bản dịch có tựa đề *A Void*, một bản dịch rất đáng đọc (xem Phụ lục A). Nếu toàn bộ cuốn sách trên bị mã hóa bằng mã thay thế dùng một bảng chữ cái thì một sự cố gắng ngây thơ nhằm giải mã nó sẽ gặp nhiều khó khăn do ở đây bị thiếu hoàn toàn chữ cái xuất hiện thường xuyên nhất trong bảng chữ cái tiếng Anh.

Dưới đây tôi sẽ đưa ra một ví dụ về sự phân tích tần suất dùng để giải mã một văn bản mã hóa. Tôi đã cố gắng tránh không đưa ra quá nhiều ví dụ về phân tích mã trong cả cuốn sách, song với phân tích tần suất thì là một ngoại lệ. Một phần là do phân tích tần suất không quá khó như ta tưởng và một phần vì nó là công cụ phân tích mã rất cơ bản. Hơn nữa, ví dụ dưới đây cho phép ta hiểu rõ quy trình làm việc của nhà phân tích mã diễn ra như thế nào. Mặc dù phân tích tần suất đòi hỏi một sự suy nghĩ logic, song bạn sẽ thấy nó cũng cần mưu mẹo, trực giác, sự linh hoạt và ước đoán.

Bảng 1 Bảng tần suất tương đối dựa trên các đoạn trích từ các báo và tiểu thuyết, với tổng số ký tự là 100.362. Bảng này do H. Beker và F.Piper biên soạn và được xuất bản lần đầu tiên trong cuốn *Các hệ thống mật mã: Sự bảo vệ thông tin*.

Chữ cái	Phần trăm
a	8,2
b	1,5
c	2,8
d	4,3
e	12,7
f	2,2
g	2,0
h	6,1
i	7,0
j	0,2
k	0,8
l	4,0
m	2,4

Chữ cái	Phần trăm
n	6,7
o	7,5
p	1,9
q	0,1
r	6,0
s	6,3
t	9,1
u	2,8
v	1,0
w	2,4
x	0,2
y	2,0
z	0,1

Phân tích một văn bản mật mã

PCQ VMJYPD LBYK LYSO KBXBJWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: "DJOXL EYPD, ICI X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJNXO X IXNCMJ CI UCMJ SXGOKLU?"

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Hãy tưởng tượng chúng ta bắt được một bức thư đã mã hóa như trên. Thách thức ở đây là phải giải mã nó. Chúng ta biết rằng văn bản này bằng tiếng Anh và nó đã được mã bằng mã thay thế dùng một bảng chữ cái, song chúng ta không biết chìa khóa mã. Kiểm tra tất cả các chìa khóa mã là điều phi thực tế, vì vậy chúng ta phải áp dụng phương pháp phân tích tần suất. Những gì dưới đây là sự hướng dẫn làm từng bước để phân tích một bản mật mã, song nếu cảm thấy tự tin thì bạn có thể bỏ qua và hãy thử tiến hành phân tích độc lập theo ý mình.

Đứng trước một bức mật mã như thế này, phản ứng tức thì của bất kỳ nhà phân tích mã nào là tiến hành phân tích tần suất của tất cả các chữ cái mà kết quả được trình bày ở Bảng 2. Không có gì đáng ngạc nhiên rằng các chữ cái có tần suất rất khác nhau. Câu hỏi đặt ra là liệu chúng ta có thể xác định được các chữ cái do chúng thay thế mà chỉ dựa vào tần suất của chúng hay không? Bản mật mã ở đây tương đối ngắn, vì vậy chúng ta không thể áp dụng dập khuôn phương pháp phân tích tần suất. Sẽ thật là ngây

thơ nếu cho rằng chữ cái thông dụng nhất trong bản mật mã, là chữ **O**, đã thay thế cho chữ cái thông dụng nhất trong tiếng Anh là chữ **e**, hay chữ cái thường xuất hiện thứ tám trong bản mật mã là chữ **Y**, đã thay thế cho chữ cái thông dụng thứ tám trong tiếng Anh là chữ **h**. Sự áp dụng phép phân tích tần suất một cách máy móc có thể sẽ dẫn đến những từ vô nghĩa. Ví dụ, từ đầu tiên **PCQ** sẽ được giải mã ra là **aov**.

Tuy nhiên, chúng ta có thể bắt đầu bằng việc lưu ý đến ba chữ cái xuất hiện hơn ba mươi lần trong bản mật mã, đó là **O**, **X** và **P**. Sẽ tương đối an toàn nếu ta giả định rằng những chữ cái thông dụng nhất trong bảng mật mã có thể là những chữ thay thế cho các chữ cái thông dụng nhất trong bảng chữ cái tiếng Anh, nhưng không nhất thiết phải theo đúng thứ tự. Nói cách khác, chúng ta không chắc chắn là **O** = **e**, **X** = **t**, và **P** = **a**, nhưng chúng ta có thể đưa ra một giả định thăm dò như sau:

O = **e**, **t** hoặc **a**, **X** = **e**, **t** hoặc **a**, **P** = **e**, **t** hoặc **a.**

Bảng 2. Phân tích tần suất của bản mật mã

Chữ cái	Tần xuất	
	Số lần xuất hiện	Phần trăm
A	3	0,9
B	25	7,4
C	27	8,0
D	14	4,1
E	5	1,5
F	2	0,6
G	1	0,3
H	0	0,0

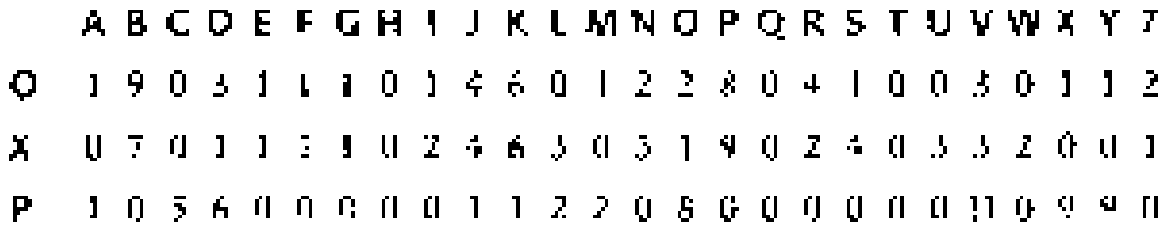
Chữ cái	Tần xuất	
	Số lần xuất hiện	Phần trăm
N	3	0,9
O	38	11,2
P	31	9,2
Q	2	0,6
R	6	1,8
S	7	2,1
T	0	0,0
Y	6	1,8

I	11	3,3
J	18	5,3
K	26	7,7
L	25	7,4
M	11	3,3

V	18	5,3
W	1	0,3
X	34	10,1
Y	19	5,6
Z	5	1,5

Để xác định rõ "hành tung" của ba chữ cái thông dụng nhất **O**, **X** và **P**, chúng ta cần một hình thức phân tích tần suất tinh vi hơn. Thay vì chỉ đơn giản đếm số lần xuất hiện của ba chữ cái, chúng ta tập trung vào việc tìm hiểu xem chúng xuất hiện bên cạnh tất cả các chữ cái khác thường xuyên tới mức nào. Ví dụ, chữ cái **O** có xuất hiện trước hay sau một vài chữ cái khác, hay nó có xu hướng chỉ đứng cạnh một số ít chữ cái đặc biệt? Trả lời câu hỏi này sẽ cho ta biết **O** là nguyên âm hay phụ âm. Nếu **O** là một nguyên âm thì nó phải đứng trước và sau hầu hết các chữ cái, còn nếu là phụ âm thì nó có xu hướng không kết hợp với nhiều chữ cái khác. Ví dụ, chữ cái **e** có thể đứng trước và sau mọi chữ cái, song chữ cái **t** lại rất ít khi thấy nó đứng trước hoặc sau các chữ cái **b, d, g, j, k, m, q** hay **v**.

Bảng dưới đây chỉ lấy ra ba chữ cái thông dụng nhất trong bản mật mã là **O, X** và **P**, và số lần nó đứng trước hay sau mỗi chữ cái. Chẳng hạn, **O** đứng trước **A** một lần, nhưng không bao giờ đứng sau nó, vì vậy tổng số sẽ là 1 ở ô thứ nhất. Chữ cái **O** đứng cạnh hầu hết các chữ cái và chỉ có 7 chữ cái nó hoàn toàn không đứng trước lẫn đứng sau, thể hiện ở bảy số 0 ở dòng **O**. **X** cũng tương đối hòa đồng, vì nó đứng cạnh hầu hết các chữ cái trừ tám chữ cái. Tuy nhiên, chữ cái **P** thì rất ít thân thiện. Nó chỉ đứng cạnh vài chữ cái, chừa ra 15 chữ cái còn lại. Bằng chứng này cho thấy **O** và **X** là nguyên âm còn **P** là phụ âm.

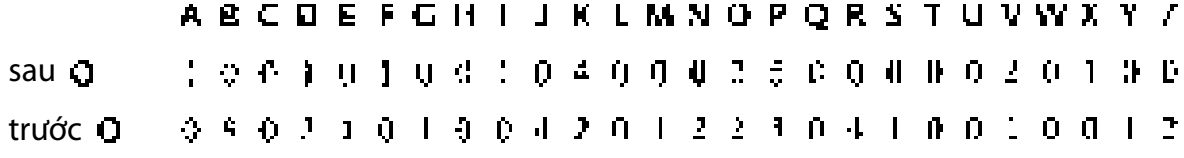


Giờ thì chúng ta phải tự hỏi nguyên âm nào đã được thay thế bằng **O** và **X**. Chúng có thể là e và a, hai nguyên âm thông dụng nhất trong tiếng Anh, nhưng **O** = **e**, và **X** = **a** hay **O** = **a** và **X** = **e**? Một đặc điểm thú vị trong bản mật mã là **OO** xuất hiện hai lần trong khi *XX* không xuất hiện lần nào. Vì các chữ cái **ee** xuất hiện nhiều hơn **aa** trong một văn bản thường bằng tiếng Anh. Do vậy chắc chắn là **O** = **e** và **X** = **a**.

Đến đây chúng ta đã xác định được chắc chắn hai chữ cái trong bản mật mã. Kết luận **X** = **a** lại càng được củng cố bởi **X** có đứng một mình trong bản mật mã và **a** (mạo từ không xác định của tiếng Anh - ND) là một trong hai từ tiếng Anh duy nhất bao gồm một chữ cái. Chữ cái còn lại trong bản mật mã đứng một mình là **Y**, và dường như chắc chắn là nó thay thế cho từ có một chữ cái còn lại trong tiếng Anh, đó là từ **i** (đại từ nhân xưng ngôi thứ nhất trong tiếng Anh - ND). Tập trung vào các từ chỉ gồm một chữ cái là một mẹo phân tích mã chuẩn, và tôi cũng đã liệt kê nó trong danh sách các điểm đặc biệt trong phân tích mã ở Phụ lục B. Mẹo này có tác dụng vì bản mật mã đang xét ở đây vẫn còn giữ nguyên dấu cách giữa các từ. Thường một người tạo mật mã sẽ bỏ hết các dấu cách để gây khó khăn hơn cho việc giải mã của đối phương.

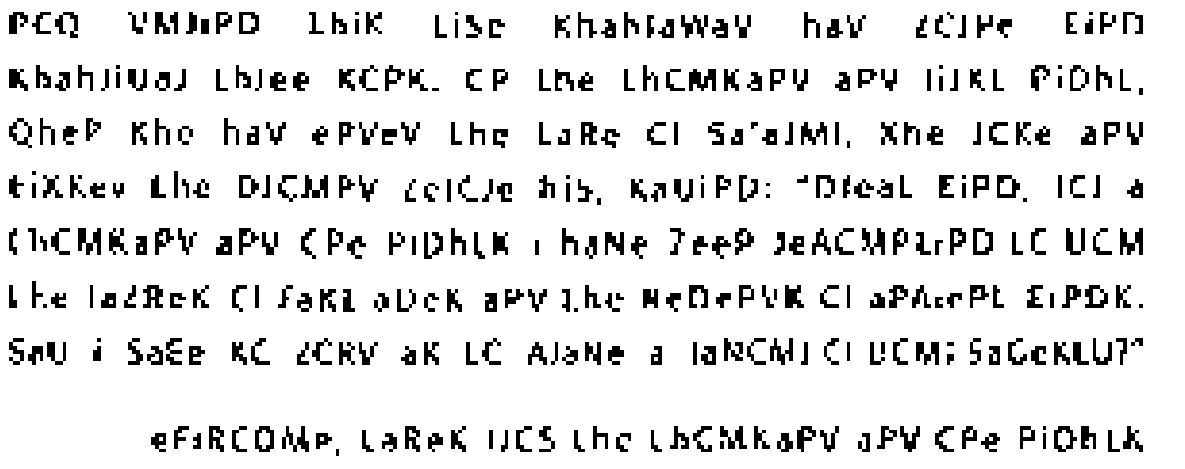
Tuy chúng ta có các dấu cách giữa các từ, song mẹo dưới đây cũng có tác dụng khi bản mật mã được viết thành một chuỗi

ký tự duy nhất. Mẹo này cho phép xác định được chữ cái **h**, một khi chúng ta đã xác định được chữ cái **e**. Trong tiếng Anh, chữ cái **h** thường đứng trước **e** (như trong các từ **the, then, they** v.v...), nhưng hiếm khi đứng sau **e**. Bảng dưới đây cho thấy chữ cái **O**, mà chúng ta đã xác định là chữ cái thay thế cho **e**, đứng trước và sau các chữ cái khác bao nhiêu lần trong bản mật mã. Bảng này gợi ý cho ta biết **B** thay thế cho **h**, vì nó đứng trước **O** chín lần nhưng lại không bao giờ đứng sau **o**. Các chữ cái khác trong bảng không có sự mất cân đối trong quan hệ với **o** đến như vậy.



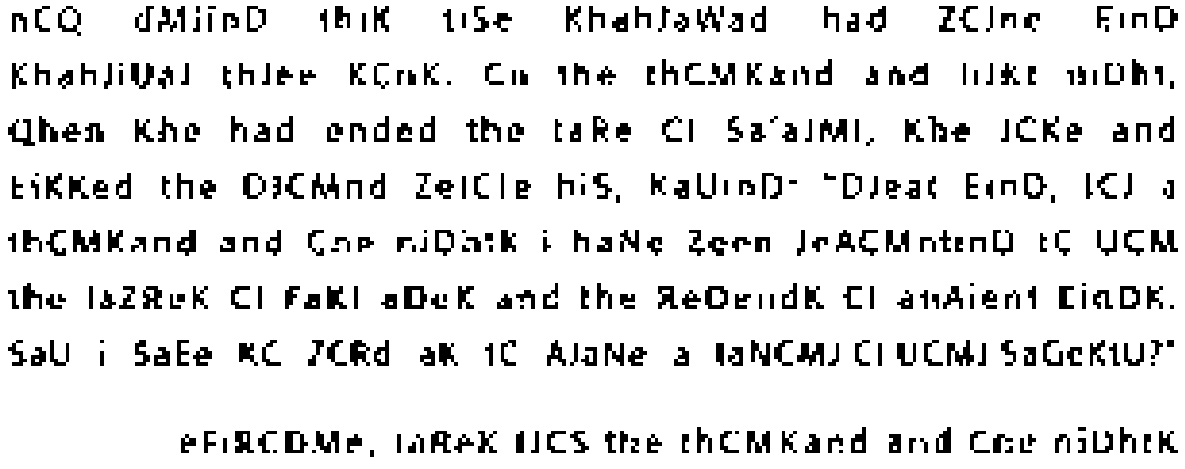
Mỗi chữ cái trong tiếng Anh đều có đặc tính của nó, trong đó bao gồm tần suất và quan hệ giữa nó với các chữ cái khác. Chính đặc tính này cho phép chúng ta xác định được đúng một chữ cái, ngay cả khi nó bị che đậy bởi phép thay thế dùng một bảng chữ cái.

Giờ chúng ta đã biết chắc chắn bốn chữ cái, **O = e, X = a, Y = i** và **B = h** và chúng ta có thể bắt đầu thay thế một số chữ cái trong bản mật mã bằng các chữ cái thường tương ứng. Tôi vẫn tuân thủ quy tắc viết các chữ cái mật mã bằng chữ in hoa còn chữ cái trong văn bản thường bằng chữ thường. Điều này giúp chúng ta phân biệt được những chữ cái đã được xác định và những chữ cái vẫn còn phải đi tìm.



eFiRCOMP, LaReK IJCS Lhe LhCMKaPV aPV CPe PiDhLK

Bước làm đơn giản này cũng giúp chúng ta xác định được thêm các chữ cái khác, bởi vì chúng ta có thể đoán được một số từ trong bản mật mã. Chẳng hạn, từ có ba chữ cái thông dụng trong tiếng Anh là **the** và **and**, và chúng có nhiều khả năng tương ứng với **-Lhe**, xuất hiện sáu lần, và **aPV** xuất hiện năm lần. Do vậy, **L** có thể là **t**, **P** có thể là **n** và **V** có thể là **d**. Giờ thì chúng ta có thể thay các chữ cái này vào bản mật mã như sau:



eFiRCOMe, IaReK IJCS the thCMKand and Cae niDhtK

Một khi một số chữ cái đã được xác định thì sự phân tích mã sẽ tiến triển rất nhanh. Chẳng hạn, từ đầu tiên của câu thứ hai là **Cn**. Mọi từ đều có nguyên âm trong đó, do vậy **C** phải là nguyên âm. Chỉ có hai nguyên âm còn chưa được xác định là **u** và **o**; **u** không thích hợp vì vậy **C** phải là **o**. Chúng ta cũng có từ

Khe, trong đó **K** chỉ có thể là **t** hoặc **s**. Nhưng vì chúng ta đã biết **L = t** nên rõ ràng là **K = s**. Như vậy ta xác định được thêm hai chữ cái nữa, thay chúng vào bản mật mã, và thấy xuất hiện cụm từ **thoMsand and one niDgts**. Ta có thể đoán ngay rằng đây là **thousand and one nights** *(Nghìn lẻ một đêm)*, và dường như chắc chắn rằng dòng cuối cùng này cho chúng ta biết đây là một đoạn trích từ truyện *Nghìn lẻ một đêm*. Điều đó có nghĩa là **M = u, I = f, J = r, D = g, R = I**, và **S = m**.

Chúng ta có thể tiếp tục thử xác định các chữ cái khác bằng việc đoán từ, song thay vì làm như vậy, chúng ta hãy xem mình đã biết được những gì về bảng chữ cái thường và bảng chữ cái mật mã. Hai bảng chữ cái đó tạo nên chìa khóa mã và chúng được sử dụng để người mã hóa thiết lập nên sự thay thế làm xáo trộn thông tin. Nhờ xác định được những chữ cái thực trong bản mật mã, giờ đây chúng ta đã có điều kiện để tìm ra những chi tiết còn lại của bảng chữ cái đó. Tóm tắt những kết quả thu được ở trên, ta có bảng chữ cái thường và bảng chữ cái mật mã dưới đây:

Bảng chữ cái thường

a b c d e f g h i j k l m n o p q r s t u v w x y z

Bảng chữ cái mật mã

X - - V O I D B Y - - R S P C - - J K L M - - - - -

Xét dãy chữ cái **VOIDBY** trong bảng chữ cái mã. Dãy này gợi ý rằng người mã hóa đã lựa chọn cụm từ chìa khóa để làm cơ sở cho chìa khóa mã. Sau một số phỏng đoán cũng đủ để biết rằng cụm từ chìa khóa có thể là **A VOID BY GEORGES PEREC**, đã được rút ngắn thành **AVOIDBYGERSPC** sau khi đã loại bỏ dấu cách và các chữ cái trùng lắp. Sau đó, các chữ cái sẽ lại tuân theo trật tự của bảng chữ cái, đồng thời bỏ đi các chữ cái đã có trong cụm từ

chìa khóa. Trong trường hợp cụ thể này người mã hóa đã thực hiện một bước khác với thông lệ là không bắt đầu cụm từ chìa khóa ở đầu của bảng chữ cái mật mã, mà lại bắt đầu sau đó ba chữ cái. Điều này có lẽ là bởi vì cụm từ chìa khóa mã bắt đầu bằng chữ **A**, và người mã hóa muốn tránh việc mã hóa **a** thành **A**. Cuối cùng, khi đã thiết lập được bảng chữ cái mật mã hoàn chỉnh, chúng ta có thể giải mã được toàn bộ bản mật mã, và việc phân tích mã đã hoàn tất.

Bảng chữ cái thường
a b c d e f g h i j k l m n o p q r s t u v w x y z
Bảng chữ cái mật mã
X Z A V O I D B Y G E R S P C F H J K L M N Q T U

> Now during this time Shahrazad had borne King Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: "Great King, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favor of your majesty?"
>
> Epilogue, *Tales from the Thousand and One Nights*

> *Giờ thì Shahrazad đã sinh hạ cho Đức Vua Shahriyar ba người con trai. Vào đêm thứ một ngàn lẻ một, khi nàng kết thúc câu chuyện về Ma'aruf, nàng bỗng nhổm dậy và hôn xuống nền đất trước mặt nhà vua và nói: "Thưa Đức vua vĩ đại, trong một ngàn lẻ một đêm, thần thiếp đã kể lại cho người những câu truyện ngụ ngôn xa xưa và những huyền thoại về các vị vua cổ đại. Thần thiếp có thể mạo muội thỉnh cầu người một đặc ân được không?"*
>
> Đoạn kết, trích từ *Nghìn lẻ một đêm*

Phục hưng ở phương Tây

Giữa năm 800 và 1200 sau CN, các học giả Ả Rập đã tận hưởng một thời kỳ huy hoàng của những thành tựu trí tuệ. Trong khi đó, châu Âu vẫn chìm đắm trong thời Trung cổ đen tối. Khi mà al-Kindī mô tả sự phát minh ra phép phân tích mã thì người châu Âu vẫn đang còn vật lộn với những cơ sở của khoa mật mã. Nơi duy nhất ở châu Âu khuyến khích việc nghiên cứu các văn bản bí mật đó là các tu viện, tại đó các tu sĩ nghiên cứu Kinh thánh để tìm kiếm những ý nghĩa ẩn giấu của nó, một niềm đam mê vẫn còn kéo dài cho đến tận thời đại ngày nay (xem Phụ lục C).

Các tu sĩ thời Trung cổ đã bị lôi cuốn vào công việc đó là bởi vì Kinh Cựu ước có chứa những ví dụ rõ ràng và chủ ý về mật mã. Chẳng hạn, Kinh Cựu ước có những đoạn được mã hóa bằng *atbash*, một dạng mã thay thế truyền thống của người Do Thái. *Atbash* bao gồm việc lấy mỗi chữ cái, đánh số vị trí của nó tính từ đầu bảng chữ cái, rồi thay thế nó bằng chữ cái ở vị trí tương ứng tính từ cuối bảng chữ cái đó. Trong tiếng Anh thì điều này có nghĩa là **a**, ở đầu bảng chữ cái, sẽ được thay thế bằng **Z**, đứng ở cuối bảng chữ cái, **b** thay bằng **Y** và cứ tiếp tục như vậy. Bản thân thuật ngữ *atbash* cũng hàm chứa trong đó phép thay thế mà nó mô tả, vì nó chứa chữ cái đầu tiên trong bảng chữ cái Hebrew, *aleph*, tiếp theo là chữ cái cuối cùng *taw*, sau đó có chữ cái thứ hai là *beth,* rồi tiếp đến chữ cái áp chót là *shin*. Một ví dụ về *atbash* có trong Sách Jeremiah 25: 26 (đoạn 25, câu 26) và 51: 41 (đoạn 51- câu 41) của Cựu ước, trong đó "Babel" được thay thế bằng từ "Sheshach", chữ cái đầu trong từ Babel là *beth*, chính là chữ cái thứ hai trong bảng chữ cái Hebrew, và nó được thay thế bằng *shin*, chữ cái thứ hai từ dưới lên; chữ cái thứ hai của từ Babel cũng là

beth và do đó nó cũng được thay bằng *shin;* chữ cuối cùng trong từ Babel là *lamed*, là chữ thứ 12 trong bảng chữ cái Hebrew, được thay thế bằng *kaph*, chữ cái thứ 12 tính từ cuối lên.

Atbash và những mật mã tương tự khác trong kinh thánh có thể chỉ có ý định làm tăng thêm sự huyền bí hơn là che giấu ý nghĩa, song chúng cũng đủ để gây sự quan tâm tới khoa học mật mã nghiêm túc. Các tu sĩ châu Âu đã bắt đầu tái khám phá những mã thay thế cũ, rồi họ cũng phát minh ra những loại mới và trong quá trình đó, họ đã góp phần làm sống lại khoa học mật mã trong nền văn minh phương Tây. Cuốn sách châu Âu được biết đến đầu tiên mô tả việc sử dụng mật mã được viết vào thế kỷ 13 bởi một tu sĩ dòng thánh Phan-xi-cô là nhà thông thái người Anh Roger Bacon. Cuốn *Thánh thư về những công trình bí mật của Nghệ thuật và sự vô dụng của Ma thuật* của ông bao gồm bảy phương pháp giữ bí mật thông tin và khuyến cáo: "Chỉ có người điên mới viết ra một điều bí mật không phải bằng cái cách có thể che giấu được những kẻ tầm thường".

Đến thứ kỷ 14, việc sử dụng mã hóa đã trở nên rộng khắp một cách nhanh chóng, với các nhà giả kim thuật và các nhà khoa học sử dụng nó để giữ bí mật những khám phá của mình. Mặc dù được biết đến nhiều hơn với những thành tựu trong văn học, song Geoffrey Chaucer cũng còn là nhà thiên văn và nhà mật mã học, ông là tác giả của một trong số những ví dụ nổi tiếng nhất về mã hóa thuở ban đầu ở châu Âu. Trong cuốn *Chuyên luận về các dụng cụ thiên văn,* ông đã đưa ra một số ghi chú bổ sung với tựa đề "Xích đạo của các hành tinh", trong đó có một vài đoạn được mã hóa. Phương pháp mã hóa của Chaucer là thay thế các chữ cái thường bằng các ký hiệu chứ không phải bằng một chữ

cái khác. Thoạt nhìn phương pháp này có vẻ như phức tạp hơn song về cơ bản cũng không khác gì so với việc thay thế chữ cái bằng chữ cái. Quá trình mã hóa và cấp độ an toàn cũng hoàn toàn như nhau.

Đến thế kỷ 15, khoa mật mã ở châu Âu đã trở thành một ngành công nghiệp rất phát triển. Sự hồi sinh của nghệ thuật và khoa học trong suốt thời kỳ Phục hưng đã tạo điều kiện cho khoa mật mã phát triển, trong khi đó sự bùng nổ những âm mưu chính trị lại là động cơ mạnh mẽ thúc đẩy sự phát triển của thông tin liên lạc bí mật. Đặc biệt là ở Italia đã hình thành một môi trường lý tưởng cho khoa mật mã. Ngoài chuyện là trái tim của thời kỳ Phục hưng, Italia còn bao gồm nhiều quốc gia độc lập nhau, mỗi quốc gia đều muốn giành ưu thế hơn so với quốc gia khác. Ngoại giao được đẩy mạnh, mỗi quốc gia đều gửi đại sứ của mình đến các quốc gia khác. Mỗi đại sứ lại thường xuyên nhận được thông tin từ cấp trên của họ, trong đó mô tả chi tiết các chính sách đối ngoại mà ông ta phải thực hiện. Đáp lại, mỗi đại sứ cũng thường xuyên gửi trở lại thông tin mà mình thu thập được. Rõ ràng là có một động cơ rất lớn để phải mã hóa thông tin ở cả hai chiều, vì vậy mỗi quốc gia đều lập ra một văn phòng mật mã và mỗi đại sứ đều có một thư ký riêng về mật mã.

Đồng thời với việc khoa học mật mã đã trở thành một công cụ ngoại giao thông thường thì khoa học phân tích mã cũng bắt đầu manh nha ở phương Tây. Bản thân các nhà ngoại giao cũng chỉ mới làm quen với các kỹ năng đòi hỏi phải có để thiết lập thông tin liên lạc an toàn, nhưng đã có sẵn những kẻ tìm cách phá hủy sự an toàn đó. Rất có thể là phép phân tích mã đã được khám phá một cách độc lập ở châu Âu, song cũng không loại trừ

khả năng nó được mang đến từ thế giới Ả Rập. Những khám phá của người Hồi giáo trong khoa học và toán học đã ảnh hưởng rất mạnh mẽ đến sự tái sinh của khoa học ở châu Âu, và phép phân tích mã cũng có thể nằm trong số những kiến thức được du nhập đó.

Có lẽ nhà phân tích mã vĩ đại đầu tiên của châu Âu là Giovanni Soro, ông được bổ nhiệm làm thư ký về mật mã cho vương triều Venice vào năm 1506. Danh tiếng của Soro được khắp Italia biết đến và những quốc gia hữu hảo vẫn gửi những bức thư họ chặn bắt được đến Venice để nhờ phân tích. Thậm chí ngay cả Vatican, có thể coi như là trung tâm phân tích mã sôi động thứ hai, cũng phải gửi cho Soro những thư tín dường như không thể thâm nhập nổi đã rơi vào tay họ. Vào năm 1526, Giáo hoàng Clement VII đã gửi đến Soro hai bức thư mật mã, và cả hai đều được gửi trở lại sau khi đã giải mã thành công. Và khi một trong những bức thư mật mã của chính Giáo hoàng bị người Florentine bắt được thì Giáo hoàng ngay lập tức đã gửi một bản sao tới cho Soro với hy vọng là ông ta sẽ khẳng định rằng nó không thể bị giải mã. Soro đã xác nhận rằng ông không thể giải được mật mã của Giáo hoàng, và điều đó có nghĩa là người Florentine cũng sẽ không thể phá nổi. Tuy nhiên, đây cũng có thể là một mánh khóe để ru ngủ những người tạo mật mã của Vatican có cảm giác sai lầm về sự an toàn - có thể Soro đã không chỉ ra những điểm yếu trong mật mã của Giáo hoàng, bởi vì nếu làm thế sẽ chỉ càng khuyến khích Vatican chuyển sang dùng một loại mật mã an toàn hơn mà Soro có thể không có khả năng phá nổi.

Ở những nơi khác của châu Âu, các cung đình cũng đã bắt đầu sử dụng các nhà phân tích mã tài năng, chẳng hạn như Philibert

Babou, nhà phân tích mã cho Vua Francis I nước Pháp. Babou nổi tiếng là nhờ sự quyết tâm đáng kinh ngạc, ông làm việc cả ngày lẫn đêm và kiên nhẫn hàng tuần để hóa giải một bức mật mã. Thật không may cho Babou, điều này đã mang lại cho nhà vua cơ hội dan díu thoải mái kéo dài với vợ ông. Cho đến cuối thế kỷ 16, sự điêu luyện trong công việc giải mã của người Pháp lại càng được củng cố với sự xuất hiện của Franois Viète, người đặc biệt thích thú giải mật mã của người Tây Ban Nha. Các nhà tạo mật mã Tây Ban Nha, những người quá ngây thơ so với các đối thủ của mình ở châu Âu, không thể tin khi phát hiện ra rằng thông tin của họ đã bị lộ hoàn toàn đối với người Pháp. Vua Philip II của Tây Ban Nha đã phải cất công tới thỉnh cầu Vatican, với lời tố cáo rằng chỉ có một cách giải thích duy nhất cho khả năng phân tích mã của Viète là ông ta là một "đại quỷ sứ trong liên minh ma quỷ". Philip cho rằng Viète phải bị xử tội trước Tòa án của Đức Hồng y giáo chủ vì hành vi tà giáo; song Giáo hoàng, người đã nhận thức rõ rằng bản thân các nhà phân tích mã của ngài cũng đang nghiên cứu mật mã Tây Ban Nha hàng năm trời, nên đã từ chối lời thỉnh cầu của người Tây Ban Nha. Tin tức về sự thỉnh cầu này đã nhanh chóng đến tai những chuyên gia mật mã ở nhiều quốc gia và các nhà mật mã Tây Ban Nha đã trở thành một trò cười của cả châu Âu.

Sự lúng túng của người Tây Ban Nha là một triệu chứng của tình trạng đối đầu giữa những nhà tạo mật mã và những nhà phân tích mã. Đây là một giai đoạn chuyển tiếp, khi mà những người tạo mật mã vẫn còn dựa vào mật mã thay thế dùng một bảng chữ cái, trong khi các nhà phân tích mã đã bắt đầu sử dụng phép phân tích tần suất để giải mã. Những người Tây Ban Nha

còn chưa thấy hết sức mạnh của phép phân tích tần suất nên vẫn tiếp tục tin tưởng vào mật mã thay thế dùng một bảng chữ cái, đồng thời còn chưa biết gì về sự mở rộng mà nhờ đó các nhà phân tích mã như Soro, Babou và Viète đã có thể đọc được thư tín của họ.

Trong khi đó, các nước đã được báo động về điểm yếu của mật mã dùng một bảng chữ cái rất nóng lòng muốn tìm kiếm một mật mã tốt hơn, có thể bảo vệ được những thông tin bí mật của quốc gia họ để các nhà phân tích mã nước khác không thể phá nổi. Một trong những cách cải tiến đơn giản nhất để tăng độ an toàn đối với mã thay thế dùng một bảng chữ cái, đó là sự đưa vào ký tự *không* (nulls), đó là những ký hiệu hoặc chữ cái không thay thế cho các chữ cái thực, mà chỉ là những chỗ trống không biểu thị cho cái gì hết. Chẳng hạn, người ta có thể thay mỗi chữ cái thường bằng một con số trong khoảng từ 1 đến 99, như vậy, có tới 73 con số không thay cho cái gì cả và chúng có thể được phân bố rải rác một cách ngẫu nhiên vào bảng chữ cái mật mã với tần suất khác nhau. Các ký tự *không* không là vấn đề gì đối với người nhận vì họ đã biết là phải bỏ qua chúng. Tuy nhiên, *nulls* lại gây khó khăn cho đối phương vì họ sẽ lúng túng lao vào phân tích tần suất. Một sự phát triển cũng đơn giản tương tự, đó là các nhà tạo mật mã đôi khi cố ý viết sai chính tả các từ trước khi mã hóa chúng. Chẳng hạn, **Thys haz thi ifekkt off diztaughting thi ballans off frikwenseas** - làm cho những người giải mã sẽ khó khăn hơn trong việc áp dụng phép phân tích tần suất. Tuy nhiên, người nhận khi biết chìa khóa mã có thể giải mã và sau đó xoay xở được với những từ viết sai chính tả nhưng không khó hiểu đó.

Một cố gắng khác để tăng cường độ an toàn cho mã thay thế dùng một bảng chữ cái là sự đưa vào các từ mã. Thuật ngữ *mã* (code) có ý nghĩa rất rộng trong ngôn ngữ hằng ngày và nó thường được sử dụng để mô tả bất kỳ một cách thức liên lạc bí mật nào. Tuy nhiên, như đã nói trong phần Mở đầu, nó cũng mang ý nghĩa cụ thể, và chỉ áp dụng cho một dạng thay thế nhất định. Cho đến giờ, chúng ta mới chỉ tập trung vào vấn đề mã thay thế, trong đó mỗi chữ cái được thay bằng một ký hiệu, một con số hoặc một chữ cái khác. Tuy nhiên, cũng có thể có sự thay thế ở mức độ cao hơn nhiều, trong đó mỗi từ được thay thế bởi một từ khác hoặc một ký hiệu, gọi là từ mã. Ví dụ:

ám sát	=	D	tướng quân	=	Σ	ngay lập tức	=	08
thư đen	=	P	vua	=	Ω	hôm nay	=	73
bắt giam	=	J	bộ trưởng	=	Ψ	đêm nay	=	28
bảo vệ	=	Z	hoàng tử	=	θ	ngày mai	=	43
Thư thường	=	**ám sát nhà vua đêm nay**						
Thư mật mã	=	**D - Ω - 28**						

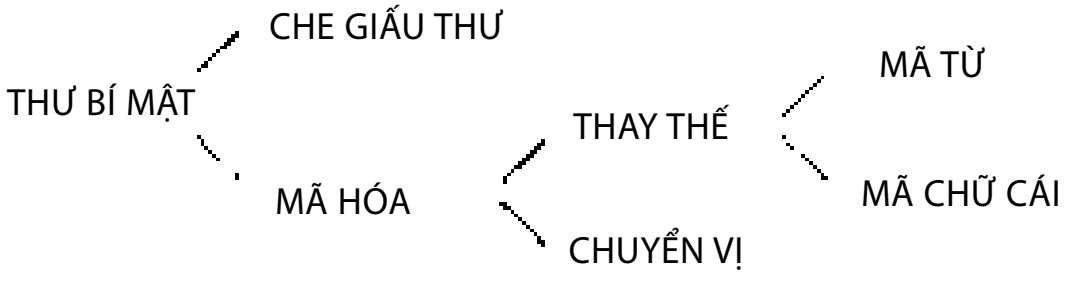
Về mặt kỹ thuật, *mã từ (code)* được định nghĩa là phép thay thế ở cấp độ từ hoặc cụm từ, trong đó *mã chữ cái (cipher)* là phép thay thế ở cấp độ chữ cái. Vì vậy, khái niệm *mã hóa chữ cái (encipher)* có nghĩa là sử dụng mã chữ cái để mã hóa một bức thư, còn *mã hóa từ (encode)* tức là mã hóa một bức thư sử dụng mã từ. Tương tự, khái niệm *giải mã chữ cái (decipher)* áp dụng cho việc giải mã một bức thư mã hóa chữ cái, còn *giải mã từ (decode)* là giải mã một bức thư dùng mã từ. Khái niệm *giải mã (decrypt)* và *mã hóa (encrypt)* thì chung hơn, nó bao gồm cả việc mã hóa và giải mã đối với cả mã từ lẫn mã chữ cái. Hình 7 trình bày tóm tắt những

định nghĩa này. Nhìn chung, tôi sẽ tuân theo những định nghĩa này song khi bối cảnh đã rõ ràng thì tôi chỉ gọi đơn giản là giải mã.

Thoạt nhìn thì mã từ có vẻ như an toàn hơn mã chữ cái vì các từ thì khó phát hiện bằng phép phân tích tần suất hơn nhiều so với mã chữ cái. Để giải mật mã dùng một bảng chữ cái, bạn cần phải xác định được giá trị (chữ cái) thực của 26 ký tự, trong khi đó để giải một mật mã từ thì bạn cần phải tìm giá trị thực của hàng trăm, thậm chí hàng nghìn từ mã. Tuy nhiên, nếu nghiên cứu mã từ một cách chi tiết hơn, ta sẽ thấy chúng có hai thiếu sót lớn về mặt thực tiễn so với mã chữ cái. Thứ nhất, một khi người gửi và người nhận đã thống nhất 26 chữ cái trong bảng chữ cái mật mã (chìa khóa mã) thì họ có thể giải mã bất kỳ thông tin nào, nhưng để có được một mức độ linh hoạt tương tự khi sử dụng mã từ thì họ phải trải qua một nhiệm vụ hết sức tỉ mỉ, đó là phải xác định được từ mã cho hàng ngàn từ khả dĩ được dùng trong văn bản thường. Sổ mã sẽ bao gồm hàng trăm trang và trông như một quyển từ điển. Nói cách khác, soạn sổ mã sẽ là một nhiệm vụ rất nặng nề và mang nó theo cũng là một sự bất tiện lớn.

Thứ hai, hậu quả của việc bị kẻ thù lấy được sổ mã là rất kinh khủng. Ngay lập tức, tất cả các thông tin được mã hóa sẽ trở nên bị lộ hết đối với kẻ thù. Người gửi và người nhận sẽ lại phải trải qua một quá trình vất vả để soạn lại một sổ mã hoàn toàn mới và bộ sách mới và nặng này sẽ phải được cung cấp cho tất cả mọi người trong mạng lưới thông tin liên lạc, điều đó có nghĩa là phải chuyển nó một cách an toàn đến mọi vị đại sứ ở mỗi quốc gia. Để so sánh, nếu kẻ thù lấy được một chìa khóa của mã chữ cái, thì sau đó ta cũng tương đối dễ dàng soạn ra một bảng chữ cái mật mã gồm 26 chữ cái mới, vừa dễ nhớ và cũng lại dễ phân phát.

Ngay ở thế kỷ 16, những người lập mật mã đã biết những điểm yếu vốn có của mã từ và vì vậy họ chủ yếu dựa vào mã chữ cái hoặc đôi khi dùng *mã hỗn hợp*. Đây là một hệ thống mã hóa trong đó chủ yếu sử dụng mã thay thế dùng một bảng chữ cái cùng với một danh sách hạn chế các từ mã. Ví dụ, một cuốn sổ mã hỗn hợp bao gồm một trang trước là bảng chữ cái mật mã và trang sau là một danh sách các từ mã. Mặc dù có thêm các từ mã, song mã hỗn hợp cũng không an toàn hơn nhiều lắm so với mã thay thế bình thường, vì phần lớn thông tin có thể bị giải mã bằng phép phân tích tần suất và phần còn lại là các từ mã có thể được đoán ra từ ngữ cảnh.



Hình 7. Khoa học viết thư tín bí mật và các nhánh chính của nó

Cũng giống như với mã hỗn hợp, các nhà phân tích mật mã giỏi nhất cũng vẫn có thể xử lý những bức thư cố ý viết sai chính tả hoặc có chứa các ký tự không *(nulls)*. Nói một cách ngắn gọn thì họ có thể hóa giải được phần lớn thư tín được mã hóa. Trình độ lão luyện của họ cho phép cung cấp một dòng thông tin ổn định lấy từ các thư tín bị giải mã, điều này có ảnh hưởng đến các quyết định của những ông chủ hay bà chủ của họ và do đó ảnh hưởng đến lịch sử của châu Âu vào những thời khắc quyết định.

Không ở đâu sự tác động của phép phân tích mã lại được minh họa một cách kịch tính hơn trường hợp của Nữ hoàng Mary xứ Scotland. Kết cục của việc xét xử bà hoàn toàn phụ thuộc vào trận chiến giữa người lập mật mã của bà và người giải mã của Nữ hoàng Elizabeth. Mary là một trong những nhân vật quan trọng nhất ở thế kỷ 16 - bà là Nữ hoàng xứ Scotland, Hoàng hậu nước Pháp và là người muốn tiếm ngôi nước Anh - song số phận của bà sẽ được quyết định chỉ bởi một mảnh giấy, với thông tin trên đó và việc nó có được giải mã hay không.

Âm mưu Babington

Vào ngày 24 tháng Mười một năm 1542, quân đội Anh của Vua Henry VIII đã đánh bại quân đội Scotland trong trận Solway Moss. Tưởng như Henry đã chinh phục được Scotland đến nơi và cướp ngôi từ tay Vua James V. Sau trận đánh, Vua Scotland quá sợ hãi đã suy sụp hoàn toàn cả về tinh thần lẫn thể xác và rút lui về cung điện ở Falkland. Ngay cả sự ra đời của con gái, Mary, chỉ hai tuần sau đó cũng không thể vực dậy nổi vị vua đau ốm. Cứ như thể ông chỉ đợi tin về đứa con thừa kế của mình để rồi có thể chết trong bình yên và tin rằng ông đã hoàn thành trách nhiệm của mình. Chỉ một tuần sau khi Mary chào đời, Vua James V đã băng hà ở tuổi 30. Công chúa ấu nhi đã trở thành Nữ hoàng Mary của Scotland.

Mary sinh thiếu tháng và ngay từ đầu người ta đã lo là cô không thể sống nổi. Những tin đồn lan sang nước Anh cho rằng đứa bé đã chết, nhưng đó chỉ là mong ước của triều đình Anh, nơi mà người ta luôn dỏng tai chờ nghe bất kỳ tin tức nào có thể làm rối loạn Scotland. Trong thực tế, Mary nhanh chóng trở

nên cứng cáp và mạnh khỏe và khi mới được 9 tháng tuổi, ngày mồng 9 tháng Chín năm 1543, cô đã lên ngôi nữ hoàng trong nhà nguyện ở Lâu đài Stirling, bao quanh là ba vị bá tước thay mặt cô cầm vương miện, vương trượng và thanh kiếm.

Thực tế Nữ hoàng Mary còn quá nhỏ đã giúp Scotland tránh được sự tấn công của nước Anh. Sẽ là không hào hiệp nếu Henry VIII lại tiến hành xâm lăng đất nước của một vị vua vừa mới băng hà và giờ đây đang được cai trị bởi một nữ hoàng tuổi còn thơ ấu. Vì vậy, vua nước Anh quyết định thực hiện chính sách lợi dụng Mary với hy vọng sẽ thu xếp một cuộc hôn nhân giữa cô và con trai ông ta, Edward, nhờ đó sẽ thống nhất hai quốc gia dưới sự trị vì của dòng họ Tudor. Ông ta bắt đầu kế hoạch của mình bằng việc thả tự do cho những hoàng thân quốc thích của Scotland bị bắt làm tù binh trong trận Solway Moss, với điều kiện họ phải tham gia chiến dịch ủng hộ cho sự hợp nhất với nước Anh.

Tuy nhiên, sau khi xem xét đề nghị của Henry, triều đình Scotland đã từ chối và chấp thuận cuộc hôn nhân của Mary với Francis, con trai cả của vua nước Pháp. Scotland lựa chọn liên minh với một quốc gia theo đạo Thiên chúa, một quyết định làm hài lòng mẹ của Mary, Mary xứ Guise, bởi lẽ chính cuộc hôn nhân của bà với Vua James V là nhằm củng cố mối bang giao giữa Scotland và Pháp. Mary và Fracis vẫn còn là những đứa trẻ, song kế hoạch cho tương lai là chúng sẽ lấy nhau và Francis sẽ lên ngôi vua nước Pháp cùng với Mary là hoàng hậu, nhờ vậy sẽ thống nhất được Scotland và Pháp. Đồng thời, Pháp cũng sẽ bảo vệ Scotland chống lại bất kỳ sự tấn công nào của nước Anh.

Lời hứa bảo vệ được tái khẳng định, nhất là khi Henry VIII đã thực hiện chính sách ngoại giao hăm dọa nhằm thuyết phục

Scotland rằng con trai ông ta mới là một chú rể xứng đáng với Nữ hoàng Mary. Quân đội của Henry đã tiến hành cướp bóc, phá hoại hoa màu, đốt cháy làng mạc và tấn công vào các thành phố và thị trấn dọc biên giới. Chính sách "tranh thủ thô bạo" như người ta vẫn gọi, vẫn tiếp tục ngay cả sau khi Henry VIII chết vào năm 1547. Dưới sự bảo hộ của con trai ông ta là Vua Edward VI (người cầu hôn), những cuộc tấn công lên đến đỉnh điểm trong trận Pinkie Cleugh khiến quân Scotland thua thảm hại. Do cuộc tàn sát này mà người ta đã quyết định, để đảm bảo an toàn, Mary phải đi Pháp, vượt ra khỏi tầm đe dọa của quân Anh, nơi cô có thể chuẩn bị cho đám cưới của mình với Francis. Ngày 7 tháng Tám năm 1548, khi mới được 6 tuổi, Mary đã phải lên thuyền dong buồm tới bến cảng Roscoff.

Những năm đầu ở Pháp của Mary có thể nói là khoảng thời gian hạnh phúc nhất trong cuộc đời cô. Được bao quanh bởi sự xa hoa và an toàn, tình yêu của cô với người chồng tương lai ngày một mặn nồng. Khi cô tròn 16 tuổi, họ lấy nhau và một năm sau, Francis và Mary trở thành Vua và Hoàng hậu của nước Pháp. Tất cả dường như đã được xếp đặt cho cuộc khải hoàn trở về Scotland của cô thì đức vua, người vốn có sức khỏe yếu ớt, đã ngã bệnh trầm trọng. Căn bệnh ở trong tai mà nhà vua mắc phải khi còn nhỏ đã trở nên xấu đi, sự viêm nhiễm đã ăn sâu vào não và nhọt bắt đầu phát triển. Năm 1560, sau chưa đầy một năm lên ngôi, Francis đã qua đời và Mary trở thành quả phụ.

Từ lúc này trở đi, cuộc đời Mary là cả một chuỗi những bi kịch. Năm 1561, bà trở về Scotland và nhận thấy đất nước đã đổi thay. Trong suốt thời gian dài vắng mặt, Mary càng củng cố đức tin Thiên chúa giáo của mình, trong khi thần dân Scotland lại

cải sang đạo Tin lành ngày càng nhiều. Mary đối xử khoan dung với ý nguyện của đại đa số dân chúng và bước đầu đã cai trị khá thành công, nhưng vào năm 1565, Mary cưới một người họ hàng của mình là Henry Stewart, Bá tước xứ Darnley, một hành động đã dẫn tới vòng xoáy suy sụp sau này. Darnley vốn là một người đàn ông thô bạo và xấu xa. Sự tham lam quyền lực một cách tàn nhẫn của ông ta đã làm mất đi sự trung thành của giới quý tộc Scotland đối với Mary. Năm sau, chính Mary đã chứng kiến bản chất dã man kinh khủng của chồng mình khi ông ta giết chết David Riccio, viên thư ký của Mary ngay trước mắt bà. Ai ai cũng thấy rõ ràng rằng vì Scotland, cần phải loại bỏ Darnley. Các nhà lịch sử hiện vẫn còn đang tranh cãi không rõ liệu Mary hay giới quý tộc Scotland chủ mưu, chỉ biết rằng đêm ngày mồng 9 tháng Hai năm 1567, ngôi nhà Darnley bị nổ tung và khi cố vùng vẫy thoát ra, ông ta đã bị bóp cổ chết. Một điều tốt lành duy nhất có được từ cuộc hôn nhân này là James, cậu con trai thừa kế.

Cuộc hôn nhân tiếp theo của Mary với James Hepburn, Bá tước thứ tư của dòng họ Bothwell, cũng chẳng tốt đẹp hơn. Mùa hè năm 1567, nhóm quý tộc Scotland theo đạo Tin lành đã hoàn toàn không còn ảo tưởng gì với vị Nữ hoàng Thiên chúa giáo của mình nữa, họ lưu đày Bothwell và bắt giam Mary, buộc bà phải từ bỏ ngai vàng cho cậu con trai mới có 14 tháng tuổi, James VI, với người em cùng cha khác mẹ với bà là Bá tước Moray làm nhiếp chính. Năm sau, Mary trốn thoát, bà bèn tập hợp lực lượng gồm 6.000 người trung thành và thực hiện nỗ lực cuối cùng nhằm đoạt lại ngai vàng. Binh lính của bà đã đối mặt với quân đội của vị nhiếp chính ở Langside, một ngôi làng nhỏ ở gần Glasgow. Mary đứng quan sát trận đánh trên đỉnh một ngọn đồi gần đó.

Mặc dù đội quân của bà áp đảo về số lượng nhưng lại thiếu kỷ luật, nên bị đánh cho tan tác. Khi biết sự thất bại là không thể tránh khỏi, bà đã bỏ trốn. Lý tưởng nhất là đi về phía đông, tới bờ biển và từ đó chạy sang Pháp, nhưng nếu như vậy thì phải vượt qua vùng đất vốn trung thành với người em trai cùng cha khác mẹ với mình, vì vậy, Mary quyết định đi về phía Nam sang nước Anh, với hy vọng người chị họ của mình là Elizabeth I có thể giúp bà lẩn trốn.

Nhưng sự đánh giá của Mary đã mắc sai lầm nghiêm trọng. Elizabeth chẳng mang lại điều gì cho Mary ngoại trừ một nhà tù khác. Lý do chính thức đưa ra cho sự bắt bớ này liên quan đến việc giết Darnley, nhưng lý do thực sự là ở chỗ Mary là mối đe dọa đối với Elizabeth, vì những người Thiên chúa giáo ở Anh coi Mary mới thực sự là nữ hoàng của nước Anh. Qua bà của mình, Margaret Tudor, người chị kế của vua Henry VIII, Mary thực sự có quyền lấy lại ngai vàng, nhưng đứa con sống sót cuối cùng của Henry là Elizabeth I dường như có quyền ưu tiên hơn. Tuy nhiên, theo những người Thiên chúa giáo, Elizabeth không thích hợp vì bà là con gái của Anne Boleyn, người vợ thứ hai của Henry sau khi ông ta ly dị Catherine của xứ Aragon, bất chấp cả Đức Giáo hoàng. Người Thiên chúa giáo ở Anh không chấp nhận sự ly dị này, họ không xác nhận cuộc hôn nhân sau của Henry với Anne Boleyn, và lại càng không chấp nhận Elizabeth, con gái của họ, là Nữ hoàng. Họ coi Elizabeth như là một đứa con hoang tiếm ngôi.

Mary bị giam cầm ở rất nhiều lâu đài và thái ấp. Tuy Elizabeth coi bà là một nhân vật nguy hiểm nhất ở nước Anh, song rất nhiều người Anh phải thừa nhận rằng họ ngưỡng mộ lối cư xử lịch lãm, sự thông minh và vẻ đẹp tuyệt vời của bà. William Cecil, quan tể

tướng của Elizabeth, đã rất có ấn tượng về "sự tiếp đãi rất quyến rũ và ngọt ngào của bà đối với tất cả các quý ông" và Nicholas White, phái viên của Cecil, cũng có nhận xét tương tự: "Bà ấy có tất cả những nét duyên dáng quyến rũ, một giọng Scotland mượt mà và một sự thông minh sâu sắc, được bao bọc bởi sự dịu dàng." Nhưng mỗi năm qua đi, trông bà càng xanh xao, sức khỏe giảm sút và bà bắt đầu mất hy vọng. Người giám sát bà, Ngài Amyas Paulet, một người Thanh giáo, hoàn toàn dửng dưng trước sự kiều diễm của bà và đối xử với bà ngày càng khắc nghiệt.

Cho đến năm 1586, sau mười tám năm giam cầm, bà đã mất tất cả đặc quyền của mình. Bà bị giam trong Lâu đài Chartley ở Staffordshire và không còn được phép đi lấy nước ở suối nước nóng Buxton, một loại nước trước đây đã giúp bà dịu bớt những cơn đau ốm thường xuyên. Trong lần cuối cùng đi đến Buxton, bà đã dùng kim cương để khắc dòng chữ sau lên một cánh cửa sổ: "Buxton, nước nóng của ngươi làm cho cái tên ngươi trở nên nổi tiếng, có lẽ ta sẽ không còn được trở lại đây nữa - Vĩnh biệt". Có vẻ như bà đã ngờ rằng mình sẽ mất nốt cả sự tự do bé nhỏ này. Nỗi buồn của Mary càng tăng thêm bởi những hành động của cậu con trai 19 tuổi, Vua James VI của Scotland. Bà vẫn luôn hy vọng một ngày nào đó, bà sẽ trốn thoát và trở về Scotland để cùng sẻ chia quyền lực với con trai mình, đứa con mà bà đã không được gặp mặt từ lúc nó mới một tuổi. Nhưng James không có chung những tình cảm như vậy với mẹ của mình. Cậu đã được kẻ thù của Mary nuôi dưỡng và dạy dỗ rằng mẹ cậu đã giết cha của cậu để cưới người bà yêu. James khinh miệt mẹ và sợ rằng nếu trở về, bà sẽ cướp lấy ngai vàng của cậu. Sự căm thù của James đối với Mary được thấy rõ qua việc cậu không hề ngần ngại cầu hôn

với Elizabeth I, người đang giam cầm mẹ cậu (và còn hơn cậu tới 30 tuổi). Nhưng Elizabeth đã từ chối lời cầu hôn này.

Mary đã viết thư cho con trai mình để thuyết phục cậu nhưng thư của bà không bao giờ tới được biên giới Scotland. Tới thời kỳ này Mary bị cô lập hơn bao giờ hết: tất cả các lá thư bà gửi đi đều bị tịch thu và mọi thư tín gửi đến cho bà đều bị cai ngục giữ lại. Tinh thần của Mary xuống thấp đến cực điểm và dường như mọi hy vọng của bà đều đã tiêu tan. Chính giữa lúc tuyệt vọng và khắc nghiệt này, ngày mồng 6 tháng Một năm 1586, bà đã nhận được một gói thư đầy bất ngờ.

Gói thư này là do những người ủng hộ Mary ở Âu lục gửi tới, và chúng được lén đưa vào ngục cho Mary bởi Gilbert Gifford, một người theo đạo Thiên chúa đã rời nước Anh từ năm 1577 và được đào tạo làm mục sư tại trường English College ở Roma. Trở về Anh năm 1585, với mong muốn được phục vụ Mary, ông ta ngay lập tức đã đến Sứ quán Pháp ở London, nơi mà thư tín (gửi cho Mary) ngày càng chất cao. Sứ quán Pháp biết rằng nếu họ chuyển những lá thư này bằng con đường thông thường thì Mary sẽ chẳng bao giờ nhìn thấy chúng. Tuy nhiên, Gifford khẳng định rằng ông ta có thể lén đưa gói thư này vào Lâu đài Chartley, và bảo đảm rằng ông ta giữ đúng lời hứa. Lần chuyển thư này là đầu tiên, nó mở đầu cho nhiều lần sau đó nữa, và Gifford trở thành một người đưa thư, không chỉ chuyển tin cho Mary mà còn chuyển cả thư phúc đáp của bà. Cách chuyển thư của Gifford vào Lâu đài Chartley quả là rất khôn khéo. Ông ta đưa thư cho một người sản xuất bia ở địa phương, người này gói chúng bằng một cái túi da, rồi giấu vào bên trong nắp rỗng đậy thùng bia. Người sản xuất bia chuyển thùng bia này đến Lâu đài Chartley,

ở đó người hầu của Mary sẽ mở nắp ra, lấy thư và đưa cho Nữ hoàng Scotland. Quy trình này cũng rất có hiệu quả để chuyển thư từ Lâu đài Chartley ra ngoài

Trong khi đó, Mary không hề biết trước rằng có một kế hoạch giải cứu bà đang được bàn bạc ở các quán trọ của London. Trung tâm của âm mưu này là Anthony Babington, tuy mới chỉ 24 tuổi nhưng đã nổi tiếng trong thành phố là một người đẹp trai, duyên dáng, dí dỏm và rất sành ăn. Điều mà rất nhiều người cùng thời hâm mộ ông không biết, đó là Babington cực kỳ căm phẫn cái guồng máy đã ngược đãi ông, gia đình ông và đức tin của ông. Những chính sách chống Thiên chúa giáo của nhà nước đã đạt đến mức độ khủng khiếp mới, các cha xứ bị buộc tội phản nghịch và bất kỳ ai bị bắt gặp chứa chấp họ đều bị trừng phạt bằng cách tra tấn, cắt xẻo các bộ phận cơ thể và mổ bụng moi ruột nếu họ vẫn còn sống. Những người Thiên chúa giáo bị cấm tụ họp và gia đình những người trung thành với Giáo hoàng bị buộc phải nộp những khoản thuế nặng nề. Sự thù hận của Babington càng tăng thêm bởi cái chết của Lãnh chúa Darcy, cụ của ông, đã bị xử chém do có liên quan đến cuộc nổi dậy của người Thiên chúa giáo chống lại Henry VIII.

Âm mưu bắt đầu vào một buổi tối tháng Ba năm 1586, khi Babington và sáu người bạn tâm giao tụ họp tại *The Plough*, một quán rượu bên ngoài đền Bar. Theo nhà lịch sử Philip Caraman, thì "Ông ta đã lôi kéo được rất nhiều người Thiên chúa giáo trẻ tuổi nhờ sức cuốn hút và nhân cách đặc biệt của ông, đó là những người có cùng địa vị, galăng, ưa mạo hiểm, dám đứng lên bảo vệ đức tin Thiên chúa trong những ngày tháng khó khăn; và sẵn sàng làm bất kỳ công việc khó khăn nào để phát triển sự nghiệp

của Thiên chúa". Sau đó vài tháng, một kế hoạch táo bạo đã được vạch ra nhằm giải thoát Nữ hoàng Mary của Scotland, ám sát Nữ hoàng Elizabeth và kích động một cuộc nổi dậy được hỗ trợ bởi một cuộc xâm lăng từ nước ngoài.

Những kẻ âm mưu cũng đã nhất trí rằng Âm mưu Babington, đó là tên mà sau này người ta gọi cuộc âm mưu này, không thể tiến hành nếu không có sự đồng ý của Mary, nhưng khốn nỗi không có cách nào để liên lạc với bà. Thế rồi, vào ngày mồng 6 tháng Bảy năm 1586, Gifford đã đến gõ cửa nhà Babington. Ông ta chuyển tới một lá thư từ Mary, giải thích rằng bà đã nghe nói về Babington qua những người ủng hộ bà ở Paris, và mong đợi tin tức từ ông. Để đáp lại, Babington đã soạn một bức thư chi tiết, trong đó ông tóm tắt kế hoạch của mình, bao gồm cả việc viện dẫn Elizabeth bị Giáo hoàng Pius V rút phép thông công từ năm 1570, mà ông tin rằng điều này sẽ hợp pháp hóa việc ám sát bà ta.

> Bản thân tôi và mười quý ông khác cùng hàng trăm người theo chúng tôi sẽ tiến hành việc cứu thoát bà khỏi tay kẻ thù. Để giết chết kẻ tiếm ngôi, do bà ta đã bị rút phép thông công khiến chúng tôi không phải tuân theo bà ta nữa, đó là sáu nhà quý tộc, tất cả đều là bạn thân tín của tôi, những người đầy nhiệt huyết với đức tin Thiên chúa và phục tùng Bệ hạ, sẽ thực hiện việc hành quyết bi thảm này.

Vẫn như trước đây, Gifford sử dụng mẹo đặt thư vào trong nắp thùng bia để lén đưa chúng qua mắt bọn lính gác của Mary. Đây có thể coi là một dạng *giấu thư*, vì lá thư đã được giấu kín. Để an toàn hơn, Babington đã mã hóa bức thư, phòng ngay cả

khi nếu bị giám ngục của Mary bắt được thì nó cũng sẽ không thể bị giải mã và âm mưu không bị bại lộ. Ông đã sử dụng mật mã chữ cái, nhưng không chỉ là mã thay thế dùng một bảng chữ cái mà là một dạng hỗn hợp, như trình bày ở Hình 8. Nó bao gồm 23 ký hiệu thay thế cho các chữ cái trong bảng chữ cái (trừ j, v và w), cùng với 35 ký hiệu biểu thị cho các từ và cụm từ. Thêm vào đó, có thêm bốn ký tự *không (nulls)* ( ) và một ký hiệu , ám chỉ ký hiệu tiếp theo biểu thị một chữ cái kép *(dowbleth)*.

Tuy tuổi còn trẻ, thậm chí còn trẻ hơn cả Babington, nhưng Gifford đã thực hiện việc chuyển thư một cách tin cậy và khôn khéo. Những bí danh của ông, như Mr. Colerdin, Pietro và Conrnelys, đã giúp ông đi lại trong nước một cách dễ dàng mà không bị nghi ngờ, đồng thời những mối liên hệ của ông trong cộng đồng những người Thiên chúa giáo đã tạo cho ông có rất nhiều ngôi nhà có thể tá túc an toàn ở London và Lâu đài Chartley. Tuy nhiên, mỗi lần đến và đi từ Charley, Gifford đều đi đường vòng. Mặc dù Gifford bên ngoài đóng vai trò là điệp viên cho Mary song ông ta thực sự là một điệp viên hai mang. Trở lại năm 1585, trước khi quay về nước Anh, Gifford đã viết thư cho Ngài Francis Walsingham, Thượng thư của Nữ hoàng Elizabeth, đề nghị xin được phục vụ ông ta. Gifford nhận thấy rằng cái mác Thiên chúa giáo của mình sẽ là một vỏ bọc hoàn hảo để dễ dàng xâm nhập vào các âm mưu chống lại Nữ hoàng Elizabeth. Trong bức thư gửi Walsingham, ông ta viết: "Tôi đã nghe nói về công việc ngài đang làm và tôi muốn được phục vụ ngài. Tôi không hề đắn đo và cũng không sợ nguy hiểm. Tôi sẽ hoàn thành bất kỳ nhiệm vụ gì ngài yêu cầu".

Hình 8. Bảng mã hỗn hợp của Nữ hoàng Mary xứ Scotland, bao gồm một bảng chữ cái mật mã và các từ mã.

Walsingham là một quan thượng thư tàn nhẫn của Elizabeth. Ông ta là một nhân vật rất xảo quyệt, một tên trùm mật thám chịu trách nhiệm về an ninh của vương quốc. Được thừa hưởng một mạng lưới điệp viên không lớn lắm, nhưng Walsingham đã nhanh chóng phát triển nó ra khắp Âu lục, nơi khởi xướng rất nhiều âm mưu chống lại Elizabeth. Sau khi Walsingham chết, người ta phát hiện ra là ông ta đã thường xuyên nhận được báo cáo từ mười hai địa điểm ở Pháp, chín ở Đức, bốn ở Italia, bốn ở Tây Ban Nha và ba ở các nước Hà Lan, Bỉ và Luxembourg cũng như có thông tin từ Constantinople, Angiêri và Tripoli.

Walsingham đã tuyển Gifford làm điệp viên và thực tế, chính Walsingham là người đã yêu cầu Gifford đến Sứ quán Pháp và xin làm người đưa thư. Mỗi lần Gifford lấy được thư gửi đến hay gửi đi từ Mary, ông ta đều mang đến cho Walsingham trước tiên. Ông trùm mật thám cáo già này, trước hết, chuyển số thư tín đó

tới những người chuyên làm giả của mình, phá xi gắn trên mỗi bức thư, sao lại một bản, gắn xi lại bằng một con dấu giả trước khi trả lại cho Gifford. Những lá thư trông rõ như là chưa bị bóc trộm này sau đó sẽ được gửi tới Mary hoặc cho những người nhận thư của bà, họ cũng như bà đều không hề hay biết những gì đang diễn ra.

Khi Gifford đưa cho Walsingham bức thư của Babington gửi cho Mary, việc trước tiên là phải giải mã nó. Walsingham trước đây cũng đã từng biết qua mật mã khi đọc một cuốn sách do nhà toán học và nhà mật mã học người Italia Girolamo Cardano viết (nhân tiện đây cũng xin nói rằng Cardano chính là người đã đề xuất một dạng chữ viết cho người mù dựa trên việc sờ bằng ngón tay, tiền thân của chữ viết Braille). Cuốn sách của Cardano đã gây được sự quan tâm đối với Walsingham, nhưng chính việc giải mã của nhà phân tích mã người Hà lan là Philip van Marnix mới thực sự khiến ông tin vào sức mạnh của việc có một người giải mã giỏi trong tay. Năm 1577, Philip ở Tây Ban Nha đã sử dụng mật mã để liên lạc với Don John ở Áo, là anh cùng cha khác mẹ và cũng là một người theo đạo Thiên chúa, có rất nhiều quyền lực ở Hà Lan. Thư của Philip mô tả một kế hoạch xâm lược nước Anh nhưng đã bị William de Orange bắt được và chuyển nó cho Marnix, viên thư ký về mật mã của ông ta. Marnix đã giải mã được kế hoạch và William đã chuyển thông tin này cho Daniel Rogers, một điệp viên Anh đang làm việc ở Âu lục, người này đã cảnh báo cho Walsingham về ý đồ xâm lược đó. Người Anh đã tăng cường bảo vệ và chừng ấy cũng đủ để ngăn chặn nó.

Giờ đây với sự nhận thức đầy đủ về giá trị của việc phân tích mã, Walsingham đã thành lập một trường mật mã ở London và

tuyển Thomas Phelippes làm thư ký về mật mã cho ông ta. Đó là một người đàn ông "có vóc dáng thấp lùn, gầy nhỏ, tóc vàng sẫm và chòm râu vàng sáng, mặt rỗ do bệnh đậu mùa để lại và cận thị, trông bề ngoài ông ta khoảng 30 tuổi". Phelippes là một nhà ngôn ngữ học, có thể nói được tiếng Pháp, Ý, Tây Ban Nha, Latin và Đức, nhưng quan trọng hơn, ông ta là một trong những nhà phân tích mã giỏi nhất châu Âu.

Mỗi lần nhận được thư từ gửi đến hoặc gửi đi từ Mary là Phelippes ngốn ngấu hóa giải. Ông ta vốn là một bậc thầy về kỹ thuật phân tích tần suất và việc tìm ra lời giải chỉ còn là vấn đề thời gian. Phelippes đã xác lập tần suất của mỗi ký tự, và những giá trị giả định cho những ký tự xuất hiện thường xuyên nhất. Khi hướng này dẫn đến sự phi lý thì ông ta quay trở lại và lựa chọn hướng thay thế khác. Dần dần rồi ông ta cũng xác định được các ký tự *null*, một tiểu xảo trong kỹ thuật mật mã và gạt chúng sang một bên. Cuối cùng, tất cả những ký tự còn lại chỉ là một nhúm các từ mã mà nghĩa của chúng có thể đoán được từ ngữ cảnh.

Khi Phelippes giải mã được bức thư của Babington gửi cho Mary, trong đó có đề xuất rõ ràng việc ám sát Elizabeth, ông ta ngay lập tức gửi bức thư đáng sợ này cho ông chủ của mình. Ngay lúc này Walsingham đã có thể bắt Babington, nhưng cái mà ông ta muốn còn lớn hơn việc xử tội chỉ một ít kẻ nổi loạn. Ông ta đợi thời cơ với hy vọng rằng Mary sẽ đáp lại và ủng hộ cho âm mưu này, nhờ đó mà có thể xử tội cả bà ta. Thực ra, Walsingham đã muốn Nữ hoàng Mary của Scotland chết từ lâu, song ông ta cũng ý thức được sự miễn cưỡng của Elizabeth trong việc trừng phạt người chị em họ của mình. Tuy nhiên, nếu ông ta có thể

chứng minh rằng Mary hậu thuẫn cho một âm mưu đe dọa mạng sống của Elizabeth thì chắc chắn là Nữ hoàng sẽ cho phép xử tội kẻ thù theo Thiên chúa giáo của mình. Hy vọng của Walsingham đã sớm được đáp ứng.

Ngày 17 tháng Bảy, Mary đã trả lời thư của Babington, chính thức ký vào bản án tử hình của chính bà. Bà đã viết một cách rõ ràng về "kế hoạch", bày tỏ mối quan tâm đặc biệt đến việc bà phải được giải thoát đồng thời hoặc trước khi ám sát Elizabeth, bởi vì nếu không, tin tức có thể đến tai gã cai ngục và hắn có thể sẽ giết chết bà. Trước khi đến tay Babington, bức thư đã được đưa đến cho Phelippes như thường lệ. Vì đã giải mã được những bức thư trước nên ông ta dễ dàng giải mã được bức thư này. Đọc xong nội dung bức thư, ông ta đánh dấu trên nó ký hiệu "Π" - biểu tượng của giá treo cổ.

Vậy là Walsingham đã có đủ bằng chứng cần có để bắt Mary và Babington, song ông ta vẫn chưa thỏa mãn. Để triệt phá âm mưu này một cách hoàn toàn, ông ta cần phải có tên của tất cả những người tham gia. Ông ta yêu cầu Phelippes viết giả mạo một đoạn tái bút vào thư của Mary, trong đó đề nghị Babington cung cấp tên của những người tham gia. Một trong những tài năng nữa của Phelippes đó là khả năng giả mạo chữ viết rất giỏi và người ta từng đồn rằng ông ta có thể "bắt chước chữ viết của bất kỳ ai, hệt như là chính tay người đó viết ra vậy, miễn là đã từng được nhìn qua một lần". Hình 9 là ảnh đoạn tái bút giả mạo đã được thêm vào bức thư của Mary gửi Babington. Nó có thể được giải mã bằng cách sử dụng bảng mã hỗn hợp của Mary, như đã được trình bày ở Hình 8, để biến thành đoạn văn thường dưới đây:

Ta rất muốn được biết tên và phẩm hạnh của sáu người sẽ thực hiện kế hoạch; bởi vì trên cơ sở hiểu biết về các thành viên, ta có thể cho ngươi thêm những lời khuyên cần thiết phải tuân theo, cũng như đôi lúc sẽ cho ngươi biết cụ thể phải tiến hành như thế nào. Cũng với mục đích đó, càng sớm càng tốt, nếu ngươi có thể, cho ta biết ai đã sẵn sàng và mọi người tham gia vào chuyện cơ mật này đã tiến hành đến đâu.

Hình 9. Đoạn tái bút giả mạo do do Thomas Phelippes thêm vào bức thư của Mary.

Mật mã của Nữ hoàng Mary xứ Scotland đã chứng minh một cách rõ ràng rằng một sự mã hóa không đủ mạnh còn tồi tệ hơn cả việc không mã hóa. Cả Mary lẫn Babington đều viết ra một cách rõ ràng những dự định của mình vì họ tin rằng sự liên lạc giữa họ là an toàn, trong khi nếu họ liên lạc một cách công khai, thì chắc rằng họ sẽ nói đến kế hoạch của mình một cách kín đáo hơn. Hơn nữa, sự tin tưởng của họ vào mật mã càng làm cho họ dễ chấp nhận sự giả mạo của Phelippes. Cả người gửi lẫn người nhận thường quá tin tưởng vào sức mạnh mật mã của họ khiến cho họ xem rằng kẻ thù không thể nhái theo mật mã và chèn thêm vào một đoạn thư giả mạo được. Sử dụng đúng một mật mã mạnh là một lợi ích rõ

ràng cho người gửi và người nhận, nhưng sử dụng sai một mật mã yếu có thể gây ra một cảm giác sai lầm về độ an toàn.

Ngay sau khi nhận được thư, Babington quyết định đi ra nước ngoài để tổ chức cuộc tấn công, và phải đăng ký tại văn phòng Bộ của Walsingham để được cấp hộ chiếu. Đây là thời điểm lý tưởng để bắt kẻ phản loạn, song viên công chức điều hành văn phòng, John Scudamore, lại không thể ngờ được rằng tên phản loạn đang bị truy nã ráo riết nhất của nước Anh lại đang hiện diện ngay trong văn phòng của mình. Không có sự trợ giúp nào, Scudamore mời Babington, người không hề nghi ngờ gì, ra một quán rượu gần đó, tranh thủ kéo dài thời gian để người của ông ta tập hợp thêm binh lính. Một lát sau, một mẩu giấy nhắn tin được chuyển đến quán rượu, thông báo cho Scudamore rằng đã đến lúc bắt tội phạm. Tuy nhiên, Babington đã thoáng trông thấy. Ông ta thản nhiên nói rằng mình cần phải trả tiền bia và bữa ăn, rồi đứng dậy, để lại kiếm và áo khoác trên bàn, ngụ ý rằng mình sẽ quay trở lại trong chốc lát. Nhưng thay vì làm vậy, ông lẻn ra cửa sau và trốn thoát, đầu tiên là tới rừng St. John, sau đó là tới Harrow. Ông ta làm mọi cách để cải trang, cắt tóc ngắn và đổi màu da bằng dầu hồ đào để che giấu vẻ ngoài quý tộc của mình. Ông đã thoát khỏi sự truy lùng trong 10 ngày, nhưng đến ngày 15 tháng Tám, ông cùng sáu người nữa đã bị bắt và đưa về London. Chuông nhà thờ đổ khắp thành phố đón mừng chiến thắng. Sự hành hình họ cực kỳ khủng khiếp. Theo nhà viết sử của Elizabeth là William Camden, "tất cả họ đều bị chặt đầu, chỗ kín bị cắt, bị moi ruột (lúc họ) còn sống và nhìn thấy, và bị phanh thây".

Trong khi đó, ngày 11 tháng Tám, Nữ hoàng Mary và tùy tùng của bà được phép có một đặc ân ngoại lệ là cưỡi ngựa trên địa

phận của lâu đài Chartley. Khi qua bãi săn bắn, Mary chợt trông thấy một nhóm người cưỡi ngựa đến gần và ngay lập tức nghĩ rằng đó là những người của Babington đến để cứu bà. Nhưng bà sớm nhận ra họ là những người đến để bắt bà chứ không phải đến để giải thoát cho bà. Mary bị dính líu vào Âm mưu Babington và bị xét xử theo Đạo luật về Hội đoàn, một Đạo luật của Quốc hội được thông qua năm 1584, nó được lập ra đặc biệt dành cho việc xử tội những ai có liên quan đến âm mưu chống lại Elizabeth.

Phiên tòa được tổ chức tại Lâu đài Fotheringhay, một nơi lạnh lẽo, u ám nằm ở giữa vùng đầm lầy hoang vu ở Đông Anglia. Nó bắt đầu vào thứ Tư, ngày 15 tháng Mười, trước sự hiện diện của hai chánh án, bốn vị quan tòa khác, Đại Chưởng ấn, người phụ trách Quốc khố, Walsingham và rất nhiều các công tước, hiệp sĩ và nam tước. Ở cuối phòng xử án, có khoảng trống dành cho người xem, đó là những người dân địa phương và người phục vụ cho hội đồng, tất cả đều háo hức chờ xem vị nữ hoàng Scotland nhún mình cầu xin sự tha thứ và nài nỉ được sống như thế nào. Tuy nhiên, Mary vẫn giữ vẻ tôn quý và bình tĩnh trong suốt phiên tòa. Sự biện hộ duy nhất của bà là từ chối bất kỳ sự liên hệ nào với Babington. "Sao tôi lại phải chịu trách nhiệm về kế hoạch phạm tội của một số người liều mạng," bà biện hộ, "họ dự định mà tôi không hề được biết hay tham gia vào?" Lời nói của bà chỉ có tác dụng nhỏ nhoi trước những bằng chứng chống lại bà.

Mary và Babington đã dựa vào một loại mật mã để giữ bí mật cho kế hoạch của mình, song họ lại đang sống trong thời đại mà khoa mật mã đã bị suy yếu bởi những tiến bộ trong kỹ thuật phân tích mật mã. Tuy mật mã của họ đủ để bảo vệ trước những kẻ nghiệp dư nhưng hoàn toàn chẳng có một cơ may nào chống lại

được một chuyên gia về phân tích tần suất. Trong phòng dành cho người xem, Phelippes ngồi lặng yên quan sát người ta đưa ra bằng chứng mà ông thu được từ những bức thư mã hóa.

Phiên tòa bước sang ngày thứ hai và Mary vẫn chối không biết gì về Âm mưu Babington. Khi phiên tòa kết thúc, bà để cho các quan tòa phán quyết số phận mình, tha thứ cho họ trước quyết định không thể thay đổi được nữa. Mười ngày sau đó, Tòa án Anh (chuyên xử kín các vụ án có liên quan tới an ninh quốc gia, đã bị giải thể vào năm 1641 - ND) đã họp lại tại Westminster và kết luận Mary phạm tội "bao che và có tư tưởng hãm hại Nữ hoàng nước Anh". Họ khuyến nghị xử tội chết và Elizabeth đã phê chuẩn bản án này.

Vào ngày 8 tháng Hai năm 1587, tại Đại sảnh của Lâu đài Fotheringhay, ba trăm khán giả đã tụ tập để chứng kiến buổi xử trảm. Walsingham cương quyết làm giảm tối đa ảnh hưởng của Mary như là một người tuẫn tiết vì đạo, ông ta đã ra lệnh phải đốt cháy bệ chém, quần áo của Mary và tất cả những gì liên quan đến cuộc hành hình để tránh việc tạo ra bất kỳ một dấu tích linh thiêng nào. Ông ta cũng dự định tổ chức tang lễ thật to cho con rể mình, Ngài Philip Sidney vào tuần sau đó. Sidney, một nhân vật anh hùng và rất nổi tiếng đã chết trong trận giao tranh với những người Thiên chúa giáo ở Hà Lan và Walsingham tin rằng một lễ diễu hành hoành tráng sẽ làm át đi sự thương cảm đối với Mary. Tuy nhiên, Mary cũng xác quyết rằng vẻ ngoài cuối cùng của bà phải đầy vẻ thách thức, cơ hội để một lần nữa khẳng định đức tin của bà với Thiên chúa giáo và khích lệ những người đi theo bà.

Trong khi tu viện trưởng của Peterborough đọc lời cầu nguyện, Mary nói lớn lời cầu nguyện của riêng bà cho sự cứu rỗi Nhà thờ Thiên chúa nước Anh, cho con trai bà và cho Elizabeth. Với

phương châm của gia đình bà, "trong sự kết thúc chính là sự bắt đầu của ta" trong tâm trí, bà đã trấn tĩnh lại và bước lên bệ chém. Những tên đao phủ đề nghị bà nói lời tha thứ và bà đáp, "Ta rộng lòng tha thứ cho các ngươi, giờ thì ta hy vọng các ngươi hãy kết thúc tất cả những phiền muộn của ta". Richard Wingfield, trong cuốn *Thuật lại những ngày cuối cùng của Nữ hoàng Scotland*, đã mô tả những khoảnh khắc cuối cùng của bà như sau:

Hình 10. Vụ hành quyết Nữ hoàng Mary xứ Scotland.

> Rồi bà ngả người xuống bệ chém một cách hoàn toàn yên lặng, duỗi dài cánh tay và chân rồi kêu lớn In manus tuas domine ba hay bốn lần, và lần cuối khi một trong hai tên đao phủ giữ bà một cách nhẹ nhàng bằng một tay, thì tên kia chém hai nhát rìu mới chặt đứt đầu bà, nhưng vì còn lại một chút xương sụn nhỏ phía sau nên lúc đó bà thốt ra một âm thanh rất nhỏ nhưng vẫn không hề xê dịch phần cơ thể nào của bà khỏi chỗ bà đã

nằm... Môi bà vẫn mấp máy gần 1/4 giờ sau khi đầu bà đã lìa khỏi cổ. Đoạn, một trong hai tên đao phủ trong khi tháo bít tất của bà đã nhìn thấy con chó nhỏ luồn ở dưới quần áo của bà mà y không thể bắt được nó xa rời cái cơ thể đã chết của chủ nó, nhưng rồi sau đó nó đi ra và nằm ở chỗ giữa đầu và vai của bà, một tình tiết còn truyền tụng lại mãi sau này.

2

Le chiffre indéchiffrable*

Trong nhiều thế kỷ, mật mã thay thế đơn giản dùng một bảng chữ cái đã đủ để bảo vệ bí mật. Sự phát triển sau đó của phương pháp phân tích tần suất, đầu tiên là ở Ả Rập và sau đó là ở châu Âu, đã phá hủy sự an toàn của nó. Cuộc hành quyết bi thảm Nữ hoàng Mary xứ Scotland là một minh chứng đầy ấn tượng cho những yếu kém của mật mã thay thế dùng một bảng chữ cái, và trong trận chiến giữa các nhà lập mã và giải mã thì rõ ràng các nhà giải mã đã thắng thế. Bất kỳ ai gửi đi một bức thư mã hóa đều phải chấp nhận rằng một chuyên gia phá mã của đối phương có thể bắt được và giải mã hầu hết những bí mật quý giá của họ.

Gánh nặng giờ đây rõ ràng đang đè lên vai các nhà lập mã. Họ phải tạo ra một loại mật mã mới, mạnh hơn, có thể đánh lừa được các nhà giải mã. Mặc dù loại mật mã này cho đến cuối thế kỷ 16 vẫn chưa xuất hiện, song nguồn gốc của nó đã có từ thời nhà thông thái xứ Florentine, thế kỷ 15, tên là Leon Battista Alberti.

---

* Tiếng Pháp: *Mật mã không thể phá nổi*

Sinh năm 1404, Alberti là một trong những nhân vật hàng đầu thời Phục hưng - ông là họa sĩ, nhà soạn nhạc, nhà thơ và triết gia, đồng thời còn là tác giả của sự phân tích khoa học đầu tiên về phối cảnh, một chuyên luận về ruồi và một bài điếu văn dành cho con chó của mình. Có lẽ ông nổi tiếng nhất là kiến trúc sư đã thiết kế Đài phun nước Trevi đầu tiên ở Rôm và viết cuốn *De re aedificatoria*, cuốn sách in đầu tiên về kiến trúc, tác phẩm có ảnh hưởng như là một chất xúc tác cho sự chuyển đổi từ kiến trúc Gothic sang kiến trúc Phục hưng.

Vào khoảng những năm 1460, khi đang đi dạo trong khu vườn của Vatican, Alberti tình cờ gặp người bạn mình là Leonardo Dato, thư ký cho giáo hoàng, và Dato đứng tán gẫu với ông về một số khía cạnh tinh tế của khoa học mật mã. Cuộc đối thoại ngẫu nhiên đó đã thôi thúc Alberti viết một tiểu luận về đề tài này, trong đó có phác thảo một thứ mà ông cho là một dạng mật mã mới. Vào thời đó, tất cả các loại mã thay thế đều đòi hỏi cần chỉ một bảng chữ cái để giải mã mỗi bức thư. Tuy nhiên, Alberti đề xuất sử dụng hai bảng chữ cái hoặc nhiều hơn, được dùng luân phiên nhau trong quá trình mã hóa, nhờ đó việc giải mã sẽ khó khăn hơn.

Bảng chữ cái thường
a b c d e f g h i j k l m n o p q r s t u v w x y z
Bảng chữ cái mật mã 1
F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Bảng chữ cái mật mã 2
G O X B F W T G Q I L A P Z J D E S V Y C R K U H N

Chẳng hạn, ở đây chúng ta có hai bảng chữ cái mật mã và chúng ta có thể mã hóa một bức thư bằng cách thay thế luân

phiên giữa chúng. Để mã hóa từ **hello,** chúng ta sẽ mã hóa chữ cái đầu tiên theo bảng chữ cái thứ nhất, như vậy **h** sẽ được thay bằng **A**, nhưng chúng ta sẽ mã hóa chữ cái thứ hai theo bảng mật mã thứ hai, như vậy **e** sẽ được thay thế bằng **F**. Để mã hóa chữ cái thứ ba, chúng ta lại sử dụng bảng chữ cái mật mã thứ nhất và chữ cái thứ tư bằng bảng mật mã thứ hai. Tức là chữ **l** thứ nhất được thay bằng **P**, chữ **l** thứ hai được thay bằng **A**. Và chữ cái cuối cùng, **o**, được thay bằng **D** theo bảng mật mã thứ nhất. Từ mã hóa cuối cùng được đọc là **AFPAD.** Lợi thế quan trọng của hệ thống mật mã Alberti là các chữ cái giống nhau trong văn bản thường không nhất thiết phải ứng với cùng một chữ cái trong văn bản mã hóa, vì vậy mỗi chữ cái **l** trong từ **hello** được mã hóa khác nhau. Tương tự, mỗi chữ cái **A** trong văn bản mã hóa biểu thị cho các chữ cái khác nhau trong văn bản thường, chữ đầu thay thế cho **h** và chữ sau cho **l**.

Mặc dù đã tình cờ chạm được vào một đột phá quan trọng bậc nhất trong suốt hơn một ngàn năm, song Alberti lại không phát triển ý tưởng của mình thành một hệ thống mã hóa hoàn chỉnh. Nhiệm vụ này đã rơi vào tay một nhóm những trí thức khác nhau, nhưng tất cả họ đều dựa trên ý tưởng ban đầu của ông. Người đầu tiên phải kể đến là Johannes Trithemius, Cha tu viện trưởng người Đức sinh năm 1462, sau đó là Giovanni Porta, một nhà khoa học người Italia sinh năm 1535 và cuối cùng là Blaise de Vigenère, một nhà ngoại giao người Pháp, sinh năm 1523. Vigenère bắt đầu làm quen với các bài viết của Alberti, Trithemius và Porta khi ông được cử sang Rôm làm công tác ngoại giao nhiệm kỳ hai năm, lúc đó ông mới 26 tuổi. Lúc đầu, sự quan tâm của ông đến khoa học mật mã chỉ đơn thuần có tính thực hành và gắn liền với công

Blaise Vigenère.

việc ngoại giao của ông. Sau đó, vào tuổi 39, Vigenère quyết định rằng ông đã kiếm đủ tiền để có thể rời bỏ con đường công danh và tập trung vào việc nghiên cứu. Chỉ lúc đó, ông mới nghiên cứu kỹ các ý tưởng của Alberti, Trithemius và Porta, biến chúng thành một dạng mật mã mới chặt chẽ và mạnh hơn.

Mặc dù Alberti, Trithemius và Porta đều đã có những đóng góp quan trọng, song mật mã này ngày nay chỉ được gọi là mật mã Vigenère để tôn vinh người đã phát triển nó đến dạng hoàn thiện cuối cùng. Sức mạnh của mật mã Vigenère là ở chỗ nó không chỉ sử dụng một mà là 26 bảng chữ cái mật mã khác nhau để mã hóa thông tin. Bước đầu tiên trong quá trình mã hóa là vẽ một bảng gọi là hình vuông Vigenère như trình bày ở Bảng 3, trong đó bảng chữ cái thường được tiếp nối bằng 26 bảng chữ cái mật mã, mỗi bảng lại dịch chuyển đi một chữ cái so với bảng chữ cái đứng ngay trước nó. Như vậy, dòng 1 biểu thị bảng chữ cái mật mã với độ dịch chuyển Ceasar là 1, tức là nó có thể được dùng để thực hiện một mã dịch chuyển Ceasar, trong đó, mỗi chữ cái trong bảng chữ cái thường được thay thế bằng chữ cái

đứng ngay sau nó. Tương tự, dòng hai biểu thị bảng chữ cái mật mã với độ dịch chuyển Ceasar là 2 và cứ tiếp tục như vậy. Dòng trên cùng của hình vuông, viết ở dạng chữ thường, biểu thị các chữ cái trong văn bản thường. Bạn có thể mã hóa mỗi chữ cái trong văn bản thường theo một trong 26 bảng chữ cái mật mã bất kỳ. Chẳng hạn, nếu sử dụng bảng mật mã số 2, thì chữ cái **a** được mã hóa thành **C**, nhưng nếu dùng bảng mật mã số 12 thì **a** được mã hóa thành **M.**

Nếu người gửi chỉ sử dụng một bảng chữ cái mật mã để mã hóa toàn bộ văn bản, thì đó chính là mã Ceasar đơn giản, một dạng mã hóa rất yếu, dễ dàng bị đối phương giải mã. Tuy nhiên, trong mã Vigenère, mỗi dòng trong hình vuông Vigenère (một bảng chữ cái riêng biệt) được sử dụng để mã hóa mỗi chữ cái trong văn bản. Nói cách khác, người gửi có thể mã hóa chữ cái đầu tiên theo dòng 5, chữ thứ hai theo dòng 14, chữ thứ ba theo dòng 21 v.v...

Để giải mã văn bản, người nhận cần phải biết dòng nào trong hình vuông Vigenère được sử dụng để mã hóa từng chữ cái, vì vậy, phải có một hệ thống chuyển đổi giữa các dòng đã được thỏa thuận từ trước. Điều này có thể thực hiện được nhờ sử dụng một từ khóa. Để minh họa cách sử dụng từ khóa với hình vuông Vigenère để mã hóa một đoạn thư ngắn, ví dụ thông báo **divert troops to east ridge** *(chuyển quân sang bờ phía đông)*, bằng cách dùng từ khóa là **WHITE**. Trước hết, từ khóa được viết bên trên đoạn thư và lặp lại liên tiếp cho đến khi mỗi chữ cái trong đoạn thư ứng với một chữ cái trong từ khóa. Văn bản mã hóa sau đó được thiết lập như sau. Để mã hóa chữ cái đầu tiên, chữ **d**, hãy xác định chữ cái của từ khóa bên trên nó, ở đây là **W**, và chữ cái

Bảng 3. Hình vuông Vigenère

này sẽ xác định dòng cụ thể trong hình vuông Vigenère. Dòng bắt đầu bằng chữ **W** là dòng 22, đây chính là bảng chữ cái mật mã sẽ được sử dụng để tìm chữ cái thay thế cho chữ **d**. Chúng ta hãy nhìn vào cột bắt đầu bằng chữ **d,** giao của cột này với dòng bắt đầu bằng chữ **W**, chính là chữ **Z**. Kết quả, chữ cái **d** trong văn bản thường được thay bằng chữ **Z** trong văn bản mã hóa.

Từ khóa
W H I T E W H I T E W H I T E W H I T E W H I
Văn bản thường
d i v e r t t r o o p s t o e a s t r i d g e
Văn bản mật mã
Z P D X V P A Z H S L Z B H I W Z B K M Z N M

Để mã hóa chữ cái thứ hai, **i**, ta lặp lại quá trình trên. Chữ cái của từ khóa ở bên trên **i** là **H**, vì vậy nó sẽ được mã hóa bằng một dòng khác trong hình vuông Vigenère: dòng bắt đầu bằng chữ **H** (dòng 7) là một bảng mật mã mới. Để mã hóa **i**, ta hãy nhìn vào cột bắt đầu bằng **i**, giao của cột này với dòng bắt đầu bằng **H**, chính là chữ **P**. Kết quả, chữ **i** trong văn bản thường được thay bằng **P**. Mỗi chữ cái trong từ khóa đều chỉ ra một bảng chữ cái mã cụ thể trong hình vuông Vigenère và vì từ khóa gồm có năm chữ cái nên người gửi sẽ mã hóa thông tin bằng cách sử dụng quay vòng năm dòng trong hình vuông Vigenère. Chữ cái thứ năm trong đoạn thư được mã hóa theo chữ cái thứ năm trong từ khóa, tức là chữ **E**, nhưng để mã hóa chữ cái thứ sáu, chúng ta lại quay trở lại chữ cái đầu tiên trong từ khóa. Một từ khóa dài hơn, hay một cụm từ khóa, sẽ sử dụng nhiều dòng hơn vào quá trình mã hóa và làm tăng mức độ phức tạp của mật mã. Bảng 4 trình bày một hình vuông Vigenère, có làm nổi rõ năm dòng (tức là năm bảng chữ cái mã) được xác định nhờ từ khóa **WHITE**.

Lợi thế lớn nhất của mật mã Vigenère, đó là nó hoàn toàn an toàn trước phương pháp phân tích tần suất đã trình bày ở Chương 1. Chẳng hạn, một nhà phân tích mật mã áp dụng phép phân tích tần suất đối với một đoạn mật mã thường bắt đầu bằng việc xác định chữ cái thông dụng nhất trong đoạn đó, trong trường hợp này là chữ **Z**, và sau đó giả định rằng nó biểu thị cho chữ cái

Bảng 4. Hình vuông Vigenère với các dòng được xác định nhờ từ khóa **WHITE**. Việc mã hóa được thực hiện bằng việc chuyển đổi giữa 5 bảng mã đã được làm nổi rõ, xác định bởi **W**, **H**, **I**, **T**, và **E**.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

thông dụng nhất trong tiếng Anh, đó là chữ **e**. Thực tế thì chữ cái **Z** biểu thị ba chữ cái khác nhau, đó là **d**, **r** và **s**, chứ không phải **e**. Đây rõ ràng là một vấn đề đối với người giải mã. Việc một chữ cái xuất hiện một vài lần trong văn bản mật mã, mỗi lần lại có

thể biểu thị một chữ cái khác nhau của văn bản thường, sẽ tạo ra một sự cực kỳ rối rắm, rất khó cho người giải mã. Một sự rắc rối tương tự, đó là một chữ cái xuất hiện vài lần trong văn bản thường lại có thể được biểu thị bởi nhiều chữ cái trong văn bản mật mã. Chẳng hạn, chữ **o** được lặp lại trong từ **troops**, được thay thế bởi hai chữ cái khác nhau - **oo** được mã hóa thành **HS**.

Đồng thời với việc không thể bị phá bởi phép phân tích tần suất, mật mã Vigenère còn có một số lượng từ khóa khổng lồ. Người gửi và người nhận có thể thỏa thuận với nhau bất kỳ một từ nào có trong từ điển, bất kỳ sự kết hợp từ nào hay thậm chí một từ do họ bịa ra. Một nhà giải mã sẽ không thể hóa giải bản mật mã bằng việc thử tất cả các từ khóa khả dĩ, đơn giản vì số lượng lựa chọn là cực kỳ lớn.

Công trình của Vigenère được trình bày hoàn chỉnh nhất trong cuốn *Traicté des Chiffres* (Chuyên luận về thư tín bí mật), được xuất bản năm 1586. Trớ trêu thay, đây lại chính là năm mà Thomas Phelippes đã phá được mật mã của Nữ hoàng Mary xứ Scotland. Ví thử thư ký của Mary đọc được chuyên luận này, ông ta sẽ biết về mật mã Vigenère, thì thư tín của Mary gửi cho Babington sẽ dễ dàng qua mặt được Phelippes và mạng sống của bà chắc đã được cứu thoát.

Vì sức mạnh và sự đảm bảo an toàn của nó, lẽ tự nhiên là mật mã Vigenère đáng ra phải được các thư ký phụ trách về mật mã đón nhận một cách nhanh chóng khắp châu Âu. Chắc hẳn là một lần nữa họ sẽ an lòng tiếp cận một dạng mã hóa an toàn mới. Nhưng ngược lại, họ có vẻ như chối bỏ mật mã Vigenère. Hệ thống rõ ràng là rất hoàn mỹ này lại gần như bị quên lãng trong suốt hai thế kỷ sau đó.

Từ sự lãng quên Vigenère đến Người Đeo Mặt Nạ Sắt

Các hình thái truyền thống của mật mã thay thế, tồn tại trước mật mã Vigenère, được gọi là mã thay thế dùng một bảng chữ cái, vì chúng chỉ sử dụng một bảng chữ cái mật mã cho một văn bản. Ngược lại, mật mã Vigenère thuộc loại được gọi là mật mã *dùng nhiều bảng chữ cái*, vì nó sử dụng một số bảng mã cho một văn bản. Bản chất nhiều bảng chữ cái trong mật mã Vigenère đã mang lại cho nó sức mạnh song cũng làm cho việc sử dụng nó trở nên phức tạp hơn. Việc phải tốn thêm công sức để thực hiện mật mã Vigenère đã làm cho rất nhiều người ngại sử dụng nó.

Đối với nhiều mục đích ở thế kỷ 17 thì mật mã thay thế dùng một bảng chữ cái đã là hoàn toàn đủ. Nếu bạn muốn đảm bảo cho những người phục vụ không thể đọc được thư từ riêng của mình, hoặc nếu muốn bảo vệ nhật ký của mình khỏi sự tọc mạch của vợ (hoặc chồng) thì dạng mật mã cổ điển này đã là lý tưởng. Sự thay thế dùng một bảng chữ cái thực hiện rất nhanh và dễ sử dụng, đủ an toàn đối với những người chưa được đào tạo bài bản về mật mã. Thực tế, mật mã thay thế dùng một bảng chữ cái đơn giản cũng đã trải qua nhiều hình thái khác nhau qua nhiều thế kỷ (xem Phục lục D). Đối với những ứng dụng quan trọng hơn, chẳng hạn như thông tin liên lạc của chính phủ và quân đội, mà độ an toàn là tối cao, thì mật mã dùng một bảng chữ cái đơn giản là chưa đủ. Những nhà tạo mã chuyên nghiệp trong cuộc chiến với các nhà giải mã cần có thứ gì đó tốt hơn, nhưng họ vẫn do dự khi lựa chọn mật mã dùng nhiều bảng chữ cái vì sự phức tạp của nó. Đặc biệt, thông tin liên lạc trong quân đội đòi hỏi phải nhanh và đơn giản, và một văn phòng ngoại giao có thể phải gửi và nhận hàng trăm thư từ mỗi ngày, vì vậy thời

gian là yếu tố rất quan trọng. Do đó, các nhà tạo mật mã cần có một dạng mật mã trung gian, khó giải mã hơn dạng mật mã dùng một bảng chữ cái nhưng lại đơn giản hơn mật mã dùng nhiều bảng chữ cái.

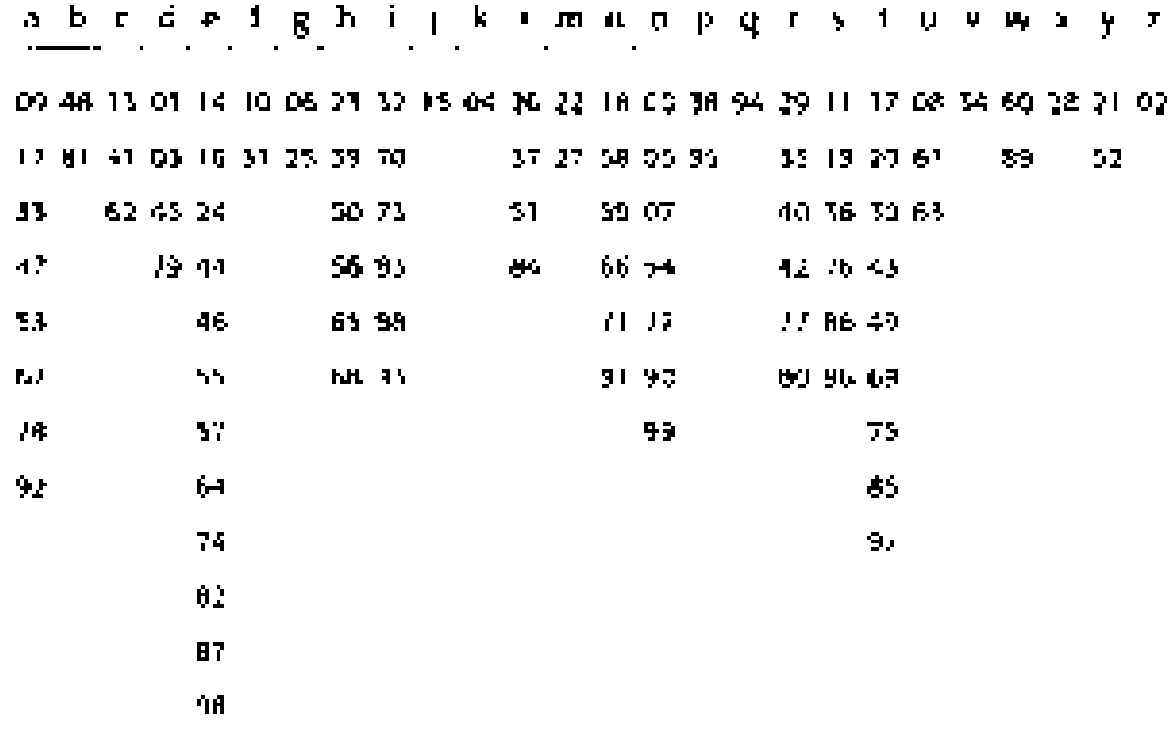
Có nhiều ứng cử viên khác nhau, trong đó *mật mã thay thế đồng âm* có hiệu quả đáng kể. Ở loại này, mỗi chữ cái được thay thế bằng nhiều lựa chọn khác nhau, số lượng các lựa chọn tiềm năng tỷ lệ với tần suất của chữ cái đó. Ví dụ, chữ **a** chiếm khoảng 8% trong chữ viết tiếng Anh và vì vậy chúng ta sẽ ấn định tám ký hiệu thay thế cho nó. Mỗi lần chữ **a** xuất hiện trong văn bản thường, nó sẽ được thay thế bằng một trong tám ký hiệu được lựa chọn ngẫu nhiên, và vì vậy cho đến cuối quá trình mã hóa thì mỗi ký hiệu chỉ chiếm khoảng 1% văn bản mật mã. Tương tự, chữ **b** chiếm 2% và chúng ta ấn định hai ký hiệu thay thế cho nó. Mỗi lần **b** xuất hiện trong văn bản thường, một trong hai ký hiệu đó sẽ được chọn để thay thế nó và kết thúc quá trình mã hóa thì nó chiếm khoảng 1%. Quá trình phân bố số các ký hiệu khác nhau cho mỗi chữ cái cứ tiếp tục cho đến hết bảng chữ cái, đến chữ **z**, rất hiếm khi xuất hiện nên chỉ một ký hiệu để thay thế nó. Trong ví dụ ở Bảng 5, các ký hiệu thay thế trong bảng mật mã là các số có hai chữ số và mỗi chữ cái trong bảng chữ cái thường có số ký hiệu thay thế nằm trong khoảng từ 1 đến 12, tùy thuộc vào độ phổ cập tương đối của mỗi chữ cái.

Chúng ta có thể nghĩ về tất cả các số có hai chữ số trong văn bản mật mã tương ứng với chữ cái **a** trong văn bản thường như là sự biểu thị hiệu quả cùng một âm, tức là âm của chữ cái **a**. Đây chính là nguồn gốc của thuật ngữ thay thế *homophonic* (thay thế đồng âm), vì *homos* có nghĩa là "cùng, đồng" và *phonos* có nghĩa

là "âm" trong tiếng Hy Lạp. Mấu chốt của việc đưa ra một số lựa chọn thay thế cho các chữ cái thông thường là nhằm cân bằng tần suất của các ký hiệu trong văn bản mật mã. Nếu chúng ta mã hóa một văn bản bằng cách sử dụng bảng mật mã ở Bảng 5 thì mỗi số chỉ chiếm khoảng 1% toàn bộ văn bản mật mã. Nếu không có ký hiệu nào xuất hiện nhiều hơn ký hiệu nào thì có vẻ như nó chống lại được bất kỳ sự tấn công nào của phép phân tích tần suất. Phải chăng khi này sẽ là tuyệt đối an toàn? Không hẳn như vậy.

Đối với một nhà giải mã thông minh thì văn bản mật mã loại này vẫn còn chứa đựng nhiều đầu mối tinh tế. Như chúng ta đã biết ở Chương 1, mỗi chữ cái trong tiếng Anh đều có đặc tính riêng, được xác định trong mối quan hệ với tất cả các chữ cái khác, và những dấu vết này vẫn có thể nhận ra, ngay cả khi mã hóa bằng mật mã thay thế đồng âm. Trong tiếng Anh, ví dụ tuyệt vời nhất về một chữ cái có đặc tính riêng biệt đó là chữ **q**, nó luôn chỉ có một chữ cái đứng sau nó, đó là **u**. Nếu thử phá một bản mật mã, ta có thể bắt đầu bằng việc lưu ý **q** là chữ cái hiếm xuất hiện và vì vậy chắc chắn nó chỉ được thay thế bằng một ký hiệu và chúng ta biết rằng **u**, được tính là chỉ chiếm khoảng 3% trong tất cả các chữ cái và có thể được thay thế bằng ba ký hiệu. Do vậy, nếu ta tìm ra một ký hiệu trong bản mật mã mà đứng sau nó luôn là ba ký hiệu riêng biệt thì có thể giả định chữ cái thứ nhất là **q** và ba ký hiệu kia là **u**. Các chữ cái khác thì khó nhận ra hơn, song cũng có thể bị lộ diện bởi mối quan hệ giữa chúng với chữ cái khác. Tuy mật mã đồng âm vẫn có thể hóa giải được song dù sao nó cũng an toàn hơn rất nhiều so với mật mã dùng một bảng chữ cái.

Bảng 5 Một ví dụ về mật mã thay thế đồng âm. Dòng đầu tiên biểu thị bảng chữ cái thường, các số bên dưới biểu thị bảng chữ cái mật mã với một số lựa chọn cho các chữ cái xuất hiện thường xuyên.



Mật mã đồng âm có vẻ giống với mật mã dùng nhiều bảng chữ cái, nhất là ở chỗ mỗi chữ cái thường có thể được mã hóa bằng nhiều cách, song cũng có một khác biệt quan trọng, và mật mã đồng âm xét cho cùng cũng chỉ là một dạng của mật mã dùng một bảng chữ cái. Trong bảng ví dụ về mật mã đồng âm trình bày ở trên, chữ cái **a** có thể được biểu thị bằng tám số. Nhưng điều quan trọng là tám số này chỉ biểu thị cho một chữ **a**. Nói cách khác, một chữ cái thường có thể được biểu thị bởi một số ký hiệu, song mỗi ký hiệu lại chỉ biểu thị cho một chữ cái. Trong mật mã dùng nhiều bảng chữ cái, một chữ cái thường cũng được biểu thị bởi nhiều ký hiệu khác nhau, nhưng còn phức tạp hơn ở chỗ, các ký hiệu này lại biểu thị nhiều chữ cái khác nhau trong cả quá trình mã hóa.

Có lẽ lý do cơ bản của việc tại sao mật mã đồng âm vẫn được xem như là mật mã dùng một bảng chữ cái là vì một khi bảng chữ cái mật mã đã được thiết lập, thì nó sẽ được duy trì trong suốt quá trình mã hóa. Việc bảng mật mã bao hàm một số lựa chọn để mã hóa một chữ cái là không quan trọng. Trong khi đó, một người sử dụng mật mã nhiều bảng chữ cái thì phải chuyển đổi liên tục giữa các bảng chữ cái khác nhau trong suốt quá trình mã hóa.

Bằng cách điều chỉnh mật mã dùng một bảng chữ cái cơ bản theo nhiều cách khác nhau, chẳng hạn như bổ sung mật mã đồng âm, nó đã trở nên an toàn hơn khi mã hóa thông tin mà không cần chuốc lấy những phức tạp của mật mã dùng nhiều bảng chữ cái. Một trong những ví dụ ấn tượng nhất về mật mã dùng một bảng chữ cái được nâng cấp đó là Mật mã Vĩ đại của Louis XIV. Mật mã Vĩ đại được sử dụng để mã hóa hầu hết các thư từ bí mật của nhà vua, bảo vệ những chi tiết trong các kế hoạch, âm mưu và chiến lược chính trị của ông. Một trong những thư từ này có đề cập đến một trong số những nhân vật bí hiểm nhất trong lịch sử nước Pháp, Người Đeo Mặt Nạ Sắt, song sức mạnh của Mật mã Vĩ đại chính là ở chỗ lá thư này và phần lớn nội dung của nó đã không bị giải mã và không thể đọc được trong suốt hai thế kỷ.

Mật mã Vĩ đại được phát minh bởi hai cha con Antoine và Bonaventure Rossignol. Antoine trở nên nổi tiếng lần đầu tiên vào năm 1626 khi ông được giao giải mã một bức thư mã hóa bắt được của một người đưa thư thoát ra từ thành phố Réalmont đang bị bao vây. Ngay trong ngày hôm đó, ông đã giải mã được bức thư, phát hiện ra rằng quân đội Huguenot* trụ trong thành

* Huguenot - người theo đạo Tin Lành (đặc biệt là ở thế kỷ 16 và 17)

phố này đang bên bờ tan rã. Người Pháp, trước đó không hề hay biết tình trạng khốn khó cùng cực của những người Huguenot, đã gửi trả lại bức thư này kèm theo bản giải mã. Người Huguenot, lúc này biết rằng kẻ thù của họ sẽ không lui quân, đã ngay lập tức đầu hàng. Bản giải mã đã làm nên một chiến thắng không đổ máu cho quân Pháp.

Sức mạnh của việc phá mã đã trở nên rõ ràng và cha con nhà Rossignols được bổ nhiệm vào các vị trí cao cấp trong triều đình. Sau khi phục vụ cho Louis XIII, họ vẫn tiếp tục là những nhà phân tích mật mã cho Louis XIV, người đã bị ấn tượng đến mức cho chuyển văn phòng của họ đến ngay cạnh khu nhà ở của mình để Rossignol, *cả cha lẫn con,* có thể đóng một vai trò trung tâm trong việc lập nên chính sách ngoại giao cho nước Pháp. Một trong những bày tỏ sự kính phục nhất đối với tài năng của họ đó là từ *rossignol* đã trở thành một từ lóng trong tiếng Pháp để chỉ dụng cụ mở khóa, ám chỉ khả năng phá khóa mã của họ.

Sự tinh xảo của Rossignol trong việc hóa giải mật mã đã mang lại cho họ sự thấu hiểu phải làm thế nào để tạo ra một dạng mã hóa mạnh hơn và họ đã phát minh ra cái gọi là Mật mã Vĩ đại. Mật mã Vĩ đại an toàn đến mức nó vô hiệu hóa mọi nỗ lực của các nhà phân tích mật mã đối phương hòng đánh cắp bí mật của nước Pháp. Thật không may, sau khi cả hai cha con họ chết đi thì Mật mã Vĩ đại cũng không được sử dụng nữa và những chi tiết chính xác của nó cũng mai một nhanh chóng, điều này có nghĩa là những giấy tờ mã hóa trong kho lưu trữ của Pháp cũng sẽ không thể đọc được nữa. Mật mã Vĩ đại mạnh đến mức nó chống lại được cả những nỗ lực của các thế hệ giải mã sau này.

Các nhà lịch sử biết rằng những giấy tờ được mã hóa bằng Mật mã Vĩ đại sẽ giúp họ hiểu rõ những âm mưu của nước Pháp thế kỷ 17, song đến tận cuối thế kỷ 19, họ vẫn không sao giải mã được chúng. Sau đó, vào năm 1890, Victor Gendron, một nhà lịch sử quân sự đang nghiên cứu những chiến dịch của Louis XIV, đã lục tìm thấy một tập mới những lá thư được mã hóa bằng Mật mã Vĩ đại. Không thể đọc nổi, ông đã chuyển chúng cho viên sĩ quan chỉ huy Étienne Bazeries, một chuyên gia xuất sắc của Cục khoa học mật mã thuộc Quân đội Pháp. Bazeries xem những lá thư này như là một thách thức tối hậu, và ông đã dành ba năm sau đó để giải mã chúng.

Những trang mã hóa bao gồm hàng ngàn con số, nhưng chỉ có 587 số khác nhau. Rõ ràng là Mật mã Vĩ đại phức tạp hơn so với mật mã thay thế đơn giản, vì mật mã thay thế chỉ đòi hỏi có 26 số khác nhau, mỗi số thay thế cho một chữ cái. Ban đầu, Bazeries nghĩ rằng các số thừa ra biểu thị các đồng âm và một vài số biểu thị cùng một chữ cái. Nghiên cứu theo hướng này, ông đã mất ba tháng nỗ lực không mệt mỏi, nhưng tất cả đều vô ích. Mật mã Vĩ đại không phải là mật mã đồng âm.

Sau đó, ông đã nghĩ ra ý tưởng là mỗi số có thể biểu diễn một cặp chữ cái, hay một *âm kép*. Chỉ có 26 chữ cái riêng biệt nhưng có đến 676 cặp chữ cái và nó gần như tương đương với số lượng các số trong bản mật mã. Bazeries thử giải mã bằng việc tìm những số xuất hiện thường xuyên nhất trong bản mật mã (**22**, **42**, **124**, **125** và **341**), giả định rằng chúng có thể là những âm kép phổ biến nhất trong tiếng Pháp **(es, en, ou, de, nt)**. Đồng thời, ông cũng áp dụng phương pháp phân tích tần suất ở cấp độ cặp chữ cái. Thật không may, lại sau vài tháng

làm việc, lý thuyết này cũng thất bại, không mang lại một bản giải mã có nghĩa nào.

Đúng lúc Bazeries sắp từ bỏ nỗi ám ảnh của mình thì một cách tấn công mới chợt nảy ra. Có lẽ ý tưởng về các âm kép cũng không xa sự thực là mấy. Ông bắt đầu để ý đến khả năng mỗi số biểu thị không phải một cặp chữ cái, mà là cả một âm tiết. Ông thử ghép mỗi số cho một âm tiết, số xuất hiện nhiều nhất có thể biểu thị cho âm tiết thông dụng nhất trong tiếng Pháp. Ông đã thử những cách hoán vị khác nhau, song tất cả đều tối nghĩa - cho đến khi ông thành công xác định được một từ. Nhóm các số (**124-22-125-46-345**) xuất hiện vài lần trong mỗi trang và Bazeries cho rằng chúng biểu thị cho **les-en-ne-mi-s**, tức là **les ennemis** (kẻ thù). Đây quả là một đột phá quan trọng.

Sau đó Bazeries đã có thể tiếp tục bằng việc xem xét các phần khác của bản mật mã, những chỗ mà các số này xuất hiện trong các từ khác. Ông đã chèn các giá trị âm tiết rút ra từ **les ennemis**, nhờ đó mà phát hiện ra các từ khác. Như những người mê chơi ô chữ đều biết, khi một từ đã được phát hiện một phần thì thường có thể đoán ra phần còn lại. Khi Bazeries hoàn thành các từ mới, ông cũng xác định được thêm nhiều âm tiết và chúng lại dẫn đến các từ khác, và cứ tiếp tục như vậy. Ông cũng thường xuyên bị vấp váp, một phần vì giá trị các âm tiết chẳng bao giờ là rõ ràng cả, một phần vì một vài số lại biểu thị cho các chữ cái riêng biệt chứ không phải là âm tiết, và một phần vì Rossignol đã đặt nhiều bẫy trong mật mã. Ví dụ, một số không biểu thị cho âm tiết cũng chẳng biểu thị một chữ cái nào, mà thay vào đó, nó lại ranh ma xóa số ở ngay trước nó.

Khi bản giải mã cuối cùng đã hoàn tất, Bazeries trở thành người đầu tiên trong vòng hai trăm năm biết đến những bí mật của Louis XIV. Tư liệu mới được giải mã này đã làm các nhà lịch sử rất phấn khởi, bởi họ đang tập trung vào một lá thư đặc biệt đã trêu ngươi họ bấy lâu. Nó dường như đã giải quyết được một trong những điều bí ẩn nhất của thế kỷ 17: đó là bộ mặt thật của Người Đeo Mặt Nạ Sắt.

Người Đeo Mặt Nạ Sắt đã là đối tượng của rất nhiều suy đoán kể từ lần đầu tiên ông bị cầm tù ở pháo đài Pignerole của Pháp ở Savoy. Khi ông bị chuyển đến Bastille năm 1698, những người nông dân đã cố tìm mọi cách để nhìn thấy mặt ông. Và họ mô tả ông cũng rất khác nhau như cao hay thấp, tóc vàng hay sẫm, trẻ hay già. Một số còn cho rằng ông là một phụ nữ. Với một vài điều xác thực, còn thì tất cả mọi người, từ Voltaire cho đến Benjamin Franklin, đều đã sáng tác ra những thuyết riêng của họ để giải thích về Người Đeo Mặt Nạ Sắt. Một thuyết đầy ẩn ý phổ biến nhất liên quan đến Mặt Nạ (ông đôi khi bị gọi tắt như vậy) cho rằng ông là anh em sinh đôi với Louis XIV, bị kết án tù để tránh mọi sự tranh cãi về ai là người có quyền chính đáng thừa hưởng ngai vàng. Một phiên bản của thuyết này cho rằng hậu duệ của Mặt Nạ vẫn còn sống sót và một dòng máu hoàng gia ẩn giấu vẫn đang tồn tại. Một cuốn sách nhỏ được xuất bản năm 1801 nói rằng chính Napoleon là một hậu duệ của Mặt Nạ, một tin đồn đã nâng cao vị thế của ông, nên vị hoàng đế này đã không hề phủ nhận.

Huyền thoại về Mặt Nạ thậm chí còn gợi cảm hứng cho thơ, văn và kịch. Năm 1848, Victor Hugo đã bắt tay viết một vở kịch nhan đề *Sinh đôi*, song khi phát hiện ra Alexandre Dumas đã lựa

chọn đề tài này nên ông đã bỏ hai hồi mà ông đã viết. Kể từ đó, cái tên của Dumas gắn liền với câu chuyện về Người Đeo Mặt Nạ Sắt. Sự thành công của cuốn tiểu thuyết này càng củng cố thêm ý tưởng cho rằng Mặt Nạ có liên quan đến nhà vua, và thuyết này vẫn dai dẳng tồn tại ngay cả khi bằng chứng được tiết lộ ở một trong những bản giải mã của Bazeries.

Bazeries đã giải mã bức thư được viết bởi Franois de Louvois, Bộ trưởng Chiến tranh của Louis XIV, mở đầu bằng việc tường thuật lại tội lỗi của Vivien de Bulonde, viên thống chế chịu trách nhiệm chỉ huy một đội quân tấn công thị trấn Cuneo, nằm ở biên giới Pháp - Ý. Mặc dù ông ta đã được lệnh giữ vững không được lui quân, song Bulonde thấy lo ngại trước những đội quân của kẻ thù tiến đến từ Áo và đã chạy trốn, bỏ lại đằng sau toàn bộ đạn dược và rất nhiều quân lính bị thương. Theo Bộ trưởng Bộ Chiến tranh, hành động này đã gây nguy hiểm cho toàn bộ chiến dịch Piedmont, và bức thư này cũng cho thấy rõ nhà vua coi hành động của Bulonde như là một hành động cực kỳ hèn nhát:

> Hoàng thượng biết rõ hơn ai hết về hậu quả của hành động này, và Ngài cũng nhận thức được sự thất bại của chúng ta trong việc chiếm lĩnh vị trí đó sẽ có tác hại sâu sắc như thế nào đến mục đích của chúng ta, một sự thất bại sẽ phải được sửa chữa trong mùa đông này. Hoàng thượng muốn ông ngay lập tức bắt giữ thống chế Bulonde và dẫn giải ông ta về pháo đài Pignerole, ở đó ông ta sẽ bị giam vào ngục có lính canh vào ban đêm và được phép đi dạo trong sân vào ban ngày với một chiếc mặt nạ.

Đây chắc chắn là nói đến người tù đeo mặt nạ ở Pignerole, và một tội lỗi cực kỳ nghiêm trọng, mà ngày tháng có vẻ như ăn khớp với huyền thoại về Người Đeo Mặt Nạ Sắt. Liệu điều đó có giải quyết được điều bí ẩn hay chưa? Không có gì đáng ngạc nhiên khi mà những người ưa thích các lời giải bí ẩn hơn đã thấy những sơ hở trong việc coi Bulonde là một ứng viên. Chẳng hạn, vẫn có ý kiến cho rằng nếu Louis XIV thực sự muốn giam giữ bí mật người anh em sinh đôi không ai biết đến của mình, thì ông ta sẽ phải để lại một loạt những dấu vết giả. Có lẽ lá thư được mã hóa này là cố ý để cho người khác giải mã. Biết đâu nhà giải mã Bazeries ở thế kỷ 19 đã bị rơi vào một cái bẫy của thế kỷ 17 cũng nên.

Phòng Đen

Việc nâng cấp mật mã dùng một bảng chữ cái bằng cách áp dụng nó cho các âm tiết hay bổ sung thêm các đồng âm có lẽ đã rất hiệu quả trong suốt những năm 1600, nhưng đến những năm 1700 thì các nhà giải mã đã trở nên công nghiệp hóa hơn, với các nhóm giải mã thuộc chính phủ cùng làm việc với nhau để hóa giải rất nhiều những bản mật mã dùng một bảng chữ cái phức tạp nhất. Mỗi cường quốc châu Âu đều có một cơ quan gọi là Phòng Đen, một trung tâm thần kinh của việc giải mã thông tin và tập hợp thông tin tình báo. Phòng Đen hiệu quả, có kỷ luật và được tán tụng bậc nhất đó là Geheime Kabinets-Kanzlei ở Vien.

Phòng này hoạt động theo một thời gian biểu nghiêm ngặt, bởi điều đó thực sự quan trọng để cho các hoạt động bất hợp pháp của nó không làm ngắt quãng sự vận hành trơn tru của dịch vụ bưu điện. Các lá thư, lẽ ra phải chuyển ngay đến các sứ

quán ở Vien, thì trước hết đều phải đi qua Phòng Đen, vào lúc 7 giờ sáng. Các thư ký làm chảy dấu niêm phong và một nhóm các nhân viên tốc ký phải đồng thời chép lại các thư tín. Nếu cần thiết, một chuyên gia về ngôn ngữ sẽ chịu trách nhiệm sao chép những bản chữ viết khác thường. Trong vòng 3 giờ đồng hồ, các lá thư lại được cho vào phong bì cũ, gắn xi và trả về bưu điện trung tâm để chúng được chuyển đến địa chỉ đã định. Những thư từ chỉ chuyển qua nước Áo thì đến Phòng Đen vào 10 giờ sáng và thư từ gửi đi từ các sứ quán ở Vien đến các địa chỉ ở ngoài nước Áo sẽ đến vào 4 giờ chiều. Tất cả thư từ đó cũng đều được sao lại trước khi được phép tiếp tục hành trình của chúng. Mỗi ngày, có tới một trăm lá thư lọc qua Phòng Đen của Vien.

Các bản sao lập tức được chuyển đến cho các nhà giải mã, họ ngồi trong những quầy nhỏ, sẵn sàng chờ giải nghĩa các bức thư. Cùng với việc cung cấp cho các hoàng đế của nước Áo những thông tin tình báo có giá trị, Phòng Đen của Vien còn bán các thông tin họ thu lượm được cho các quốc gia khác ở châu Âu. Vào năm 1774, một cuộc mua bán đã được thực hiện với Abbot Georgel, bí thư của Sứ quán Pháp, trong đó, ông ta có được trọn gói thông tin hai tuần liền với giá 1.000 đồng tiền vàng. Sau đó ông ta đã gửi thẳng những lá thư trong đó có chứa những kế hoạch bí mật của nhiều quốc gia cho Louis XV ở Paris.

Phòng Đen đã làm cho tất cả các dạng của mật mã dùng một bảng chữ cái trở nên không an toàn. Đối mặt với những đối thủ giải mã chuyên nghiệp như vậy, các nhà tạo mật mã cuối cùng đã buộc phải lựa chọn mật mã an toàn nhưng phức tạp hơn, đó là mật mã Vigenère. Dần dần, các thư ký về mật mã bắt đầu chuyển sang sử dụng các mật mã dùng nhiều bảng chữ cái. Ngoài việc

phân tích mật mã có hiệu quả hơn, còn có thêm một áp lực nữa khuyến khích việc chuyển sang dạng mã hóa an toàn hơn: đó là sự phát minh ra máy điện báo và sự cần thiết phải bảo vệ các bức điện tín không bị chặn bắt và giải mã.

Mặc dù máy điện báo, cùng với cuộc cách mạng viễn thông sau đó, ra đời vào thế kỷ 19, song có thể coi nguồn gốc của nó đã có từ năm 1753. Một bức thư vô danh trên một tạp chí Scotland đã mô tả phương pháp gửi thư qua khoảng cách rất xa bằng cách nối giữa người gửi và người nhận 26 sợi dây cáp, mỗi dây được dùng cho một chữ cái trong bảng chữ cái. Người gửi có thể chuyển đi từng chữ cái trong một bức thư bằng cách gửi đi những xung điện dọc theo mỗi đường dây. Chẳng hạn, để chuyển đi chữ **hello**, người gửi phải bắt đầu gửi đi một tín hiệu qua đường dây **h**, sau đó là đường dây **e** và cứ tiếp tục như vậy. Người nhận bằng cách nào đó cảm nhận được dòng điện đến ở mỗi dây và đọc được thư. Tuy nhiên, "phương pháp truyền tải thông tin mau lẹ" này, như người phát minh ra nó đã gọi như vậy, chưa bao giờ được thiết lập, bởi vì có một số trở ngại về mặt kỹ thuật cần phải vượt qua.

Chẳng hạn, các kỹ sư cần phải có một hệ thống đủ nhạy để bắt các tín hiệu điện. Ở Anh, Ngài Charles Wheatstone và William Fothergill Cooke đã chế tạo các máy dò từ các kim từ tính, chúng bị đổi hướng mỗi khi có sự hiện diện của dòng điện. Đến năm 1839, hệ thống của Wheatstone và Cooke đã được sử dụng để gửi thư giữa các ga xe lửa ở West Drayton và Paddington, cách nhau 29 km. Tiếng tăm về máy điện báo và tốc độ truyền tin đáng kể của nó nhanh chóng lan xa và không gì có thể quảng bá cho sức mạnh của nó hơn là truyền tin về sự chào đời đứa con trai

thứ hai của Nữ hoàng Victoria, Hoàng tử Alfred, ở Windsor vào ngày 6 tháng Tám năm 1844. Tin tức về sự ra đời của Hoàng tử đã được đánh điện tới London, và trong vòng một giờ, tờ *Thời báo* đã rải khắp các đường phố thông báo về tin vui này. Tờ *Thời báo* tuyên bố lập được chiến công này chính là nhờ công nghệ và nhấn mạnh rằng nó đã "mắc nợ sức mạnh phi thường của máy điện báo điện-từ". Ngay năm sau, máy điện báo lại có thêm danh tiếng khi nó hỗ trợ cho việc bắt giữ John Tawell, người đã giết bà chủ nhà của mình ở Slough và đã cố tình bỏ trốn bằng cách nhảy lên một chuyến tàu đi London. Cảnh sát địa phương đã đánh điện đến London mô tả về Tawell và anh ta đã bị bắt ngay khi vừa tới Paddington.

Trong khi đó ở Mỹ, Samuel Morse cũng vừa chế tạo đường dây điện báo đầu tiên của mình, một hệ thống kéo dài 60 km giữa Baltimore và Washington. Morse đã sử dụng một máy điện từ để tăng cường tín hiệu, nhờ đó khi đến phía người nhận, nó đủ mạnh để tạo nên một chuỗi các vạch ngắn và dài, đó là dấu chấm (.) và dấu gạch (-) trên một mẩu giấy. Ông cũng đã phát minh ra mã Morse quen thuộc ngày nay để chuyển mỗi chữ trong bảng chữ cái thành các dấu chấm và dấu gạch, như trình bày ở Bảng 6. Để hoàn thiện hệ thống của mình, ông đã thiết kế một cái máy nghe để người nhận có thể nghe được mỗi chữ cái như là một chuỗi các dấu chấm và dấu gạch.

Trở lại châu Âu, tiến bộ của Morse đã dần thay thế cho hệ thống Wheatstone-Cooke, và vào năm 1851, một dạng mã Morse của châu Âu, trong đó bao gồm cả các chữ cái có trọng âm, đã được đón nhận khắp châu lục. Mỗi năm qua đi, mã Morse và máy điện báo lại có một ảnh hưởng ngày càng lớn đến thế giới,

cho phép cảnh sát bắt được nhiều tội phạm hơn, giúp cho các tờ báo mang đến thông tin nóng hổi hơn, cung cấp thông tin có giá trị cho các doanh nghiệp và cho phép các công ty ở xa nhau có thể giao dịch tức thời.

Tuy nhiên, việc bảo vệ những thông tin thường là nhạy cảm này là một mối lo ngại lớn. Bản thân mã Morse không phải là một hình thức mã hóa, vì nó không che giấu thông tin. Các dấu chấm và dấu gạch chỉ là một cách thuận tiện để biểu thị các chữ cái qua môi trường điện báo; mã Morse đơn thuần chỉ là một dạng khác của bảng chữ cái mà thôi. Vấn đề an toàn nổi lên hàng đầu bởi vì không ai lại muốn gửi đi một bức thư mà lại phải đưa cho một nhân viên đánh mã Morse đọc nó để chuyển đi cả. Những nhân viên điện báo phải đọc tất cả thư từ và vì vậy sẽ có rủi ro nếu như một công ty nào đó mua chuộc được họ để tiếp cận những thông tin của đối phương. Vấn đề này đã được nêu trong một bài báo về điện báo xuất bản năm 1853 trên tờ *Quarterly Review* ở Anh:

> Lẽ ra người ta đã phải có biện pháp để ngăn ngừa sự phản đối gay gắt, hiện đang được cảm thấy đối với việc gửi những thông tin riêng tư bằng điện báo - một sự xâm phạm trắng trợn đến mọi bí mật - bất kể là thế nào cũng có đến nửa tá người hiểu được mọi từ mà người này viết cho người khác. Nhân viên Công ty Điện báo Anh đã thề giữ bí mật, nhưng một điều không thể dung thứ được, là chúng ta phải chứng kiến ngay trước mắt cảnh người lạ đọc được những điều mà chúng ta vừa viết ra. Đây là một sai sót trầm trọng trong điện báo và nó phải được sửa chữa bằng mọi cách.

Bảng 6 Các ký hiệu mã Morse quốc tế

Ký hiệu	Mã	Ký hiệu	Mã
A	· –	W	· – –
B	– · · ·	X	– · · –
C	– · – ·	Y	– · – –
D	– · ·	Z	– – · ·
E	·	O	– – – – –
F	· · – ·	1	· – – – –
G	– – ·	2	· · – – –
H	· · · ·	3	· · · – –
I	· ·	4	· · · · –
J	· – – –	5	· · · · ·
K	– · –	6	– · · · ·
L	· – · ·	7	– – · · ·
M	– –	8	– – – · ·
N	– ·	9	– – – – ·
O	– – –	Dấu .	· – · – · –
P	· – – ·	Dấu ,	– – · · – –
Q	– – · –	Dấu ?	· · – – · ·
R	· – ·	Dấu :	– – – · · ·
S	· · ·	Dấu ;	– · – · – ·
T	–	Dấu -	– · · · –
U	· · –	Dấu /	– · · – ·
V	· · · –	Dấu “	· – · · –

Giải pháp ở đây là phải mã hóa thư tín trước khi đưa nó cho điện báo viên. Điện báo viên sẽ chuyển bản mật mã này thành mã Morse trước khi truyền đi. Đồng thời với việc ngăn không cho điện báo viên đọc được những thông tin nhạy cảm, việc mã hóa còn ngăn chặn được những mưu toan của bất kỳ thám tử nào định ghi âm lại từ đường dây điện báo. Mật mã dùng nhiều

bảng chữ cái của Vigenère rõ ràng là cách tốt nhất để bảo đảm an toàn cho những thông tin kinh doanh quan trọng. Nó được xem như một mật mã là không thể giải nổi, và được biết đến dưới cái tên *le chiffre indéchiffrable* (mật mã không thể phá nổi). Các nhà tạo mã rõ ràng là đã, ít nhất là trong lúc này, dẫn trước các nhà giải mã.

Babbage và Mật mã Vigenère

Một nhân vật gợi sự hiếu kỳ nhất trong lĩnh vực phân tích mật mã thế kỷ 19 đó là Charles Babbage, một thiên tài lập dị người Anh, người nổi tiếng nhất vì đã phát minh ra bản thiết kế máy tính hiện đại. Ông sinh năm 1791, là con trai của Benjamin Babbage, một ông chủ ngân hàng giàu có ở London. Vì lấy vợ mà không được sự chấp thuận của cha, nên Charles không được hưởng tài sản giàu có của gia đình Babbage, song ông vẫn có tiền đủ để an toàn về phương diện tài chính và ông đã theo đuổi cuộc đời của một học giả lang thang, sử dụng trí tuệ của mình cho bất kỳ vấn đề nào khiến ông thích thú. Những phát minh của ông bao gồm đồng hồ đo tốc độ và máy xua đuổi bò, một thiết bị gắn trước đầu máy xe lửa để đuổi gia súc ra khỏi đường ray. Xét ở giác độ đột phá khoa học thì ông là người đầu tiên nhận ra độ rộng của tán cây phụ thuộc vào thời tiết trong năm, và ông đã suy luận rằng có thể xác định được các vùng khí hậu trong quá khứ bằng cách nghiên cứu các cây cổ thụ. Ông cũng rất ham mê môn thống kê và như là một kiểu giải trí, ông đã lập ra một tập hợp các bảng về tỷ lệ tử vong, một công cụ cơ bản cho lĩnh vực bảo hiểm ngày hôm nay.

Babbage không chỉ đóng khung trong việc giải quyết các vấn đề về khoa học và kỹ thuật. Chi phí cho việc gửi thư thường được tính toán dựa trên khoảng cách giữa nơi gửi và nơi nhận, song Babbage đã chỉ ra rằng chi phí lao động cần cho việc tính toán giá mỗi bức thư còn lớn hơn cả bưu phí. Vì vậy, ông đã đề xuất hệ thống mà chúng ta vẫn còn sử dụng cho đến ngày nay, tức là chỉ áp dụng một giá duy nhất cho tất cả các bức thư, bất kể địa chỉ gửi đến là ở đâu trong nước. Ông cũng rất quan tâm đến các vấn đề chính trị và xã hội, và đến tận lúc cuối đời, ông vẫn bắt đầu một chiến dịch dẹp bỏ những người chơi đàn organ quay tay và những nghệ sĩ đường phố lang thang khắp London. Ông phàn nàn rằng loại âm nhạc này "đôi khi khơi nguồn cho lũ trẻ con ăn mặc rách rưới và có khi cả những gã nửa say nửa tỉnh nhảy múa, hò hét ầm ĩ chói tai. Một tầng lớp khác cổ vũ nồng nhiệt cho thứ âm nhạc đường phố này bao gồm những phụ nữ đức hạnh đáng ngờ và ham chạy theo xu hướng thị thành, nó mang lại cho họ cơ hội vứt bỏ sự đoan trang để phô bày vẻ hấp dẫn của mình bên cửa sổ mở toang". Không may cho Babbage, các nghệ sĩ đã trả đũa lại bằng cách tụ tập thành một nhóm lớn quanh nhà ông và chơi nhạc thật to.

Bước ngoặt trong sự nghiệp khoa học của Babbage là vào năm 1821, khi ông và nhà thiên văn học John Herschel tiến hành xem xét lại một tập hợp các bảng biểu toán học, được sử dụng làm cơ sở cho những tính toán trong thiên văn, kỹ thuật và hàng hải. Hai người đã cực kỳ khó chịu trước số lượng các sai sót trong các bảng biểu này, chúng có thể gây ra những sai lầm trong các tính toán quan trọng. Một tập các bảng biểu có tên là *Cẩm nang hàng hải để xác định vĩ độ và kinh độ trên biển*, có chứa tới hơn

một nghìn lỗi. Thực sự thì rất nhiều vụ đắm tàu và các thảm họa kỹ thuật là do những bảng biểu có nhiều sai sót này.

Thực ra, các bảng biểu toán học này đều được tính toán bằng tay nên những sai sót đơn giản là kết quả của những nhầm lẫn rất con người. Điều này khiến cho Babbage phải thốt lên "Cầu Chúa để cho những tính toán này được thực hiện bằng máy hơi nước!". Điều này đã đánh dấu cho sự khởi đầu của một nỗ lực phi thường nhằm chế tạo ra một loại máy có thể tính toán không sai sót các bảng biểu với độ chính xác cao. Vào năm 1823, Babbage đã thiết kế "Máy Sai Phân số 1", một máy tính khổng lồ có chứa tới 25.000 bộ phận chính xác, được chế tạo bằng tiền do chính phủ tài trợ. Mặc dù Babbage là một nhà phát minh đại tài song ông lại không phải là một người thực thi vĩ đại. Sau 10 năm làm việc vất vả, ông đã từ bỏ "Máy Sai Phân số 1", lập một thiết kế hoàn toàn mới và tiến hành chế tạo "Máy Sai Phân số 2".

Khi Babbage từ bỏ cái máy đầu tiên của mình, chính phủ đã không còn tin tưởng vào ông nữa và quyết định cắt kinh phí cho nó bằng việc rút ra khỏi dự án mà nó đã tiêu tốn hết 17.470 bảng Anh, đủ để chế tạo được hai tàu chiến. Có lẽ cũng chính vì việc cắt tài trợ này đã khiến Babbage sau đó đã than phiền rằng: "Hãy cứ đề xuất với một người Anh bất kỳ nguyên lý nào, hay công cụ nào, dù có được khâm phục đi nữa, bạn sẽ thấy toàn bộ những nỗ lực của trí tuệ nước Anh đều chỉ nhằm tìm ra những khó khăn, khiếm khuyết hay sự bất khả thi trong đó. Nếu bạn nói với ông ta về một cái máy có thể gọt được vỏ khoai tây, ông ta sẽ tuyên bố là không thể tin được: nếu bạn gọt khoai tây ngay trước mặt ông ta, ông ta sẽ nói là vô dụng vì nó không thể cắt lát quả dứa".

Thiếu đi vốn tài trợ của chính phủ đồng nghĩa với việc Babbage không bao giờ hoàn thành được Máy Sai Phân số 2. Bi kịch khoa học chính là ở chỗ máy tính của Babbage lẽ ra phải là một bước đệm dẫn đến Máy Phân Tích, một loại máy có thể lập trình được. Không chỉ tính toán một số loại bảng biểu cụ thể mà Máy Phân Tích còn có thể giải quyết được nhiều bài toán toán học tùy thuộc vào các lệnh đã cho. Quả thực, Máy Phân Tích đã cung cấp một khuôn mẫu cho các máy tính hiện đại. Thiết kế của nó bao gồm một "kho lưu trữ" (bộ nhớ) và một "nhà máy xay" (bộ phận xử lý), cho phép nó đưa ra các quyết định và lặp lại các lệnh, tương đương như lệnh "**if... then...**" và "**loop**" (vòng lặp) trong các lập trình máy tính hiện đại.

Charles Babbage

Mãi một thế kỷ sau, trong suốt thời kỳ Chiến tranh Thế giới thứ II, những hiện thân điện tử đầu tiên của máy tính Babbage đã có ảnh hưởng sâu sắc đến lĩnh vực phân tích mật mã, song sinh thời, ông còn có một đóng góp quan trọng không kém cho ngành giải mã: đó là ông đã thành công phá được mật mã Vigenère mà nhờ đó, ông đã tạo được một đột phá vĩ đại nhất trong lịch sử

phân tích mật mã kể từ sau khi các học giả Ả Rập giải được mật mã dùng một bảng chữ cái nhờ phát minh ra phương pháp phân tích tần suất ở thế kỷ thứ 9. Thành công của Babbage không cần đến những tính toán bằng máy móc hay những loại máy tính phức tạp mà chỉ hoàn toàn bằng sự khôn khéo.

Babbage thích mật mã từ khi còn rất ít tuổi. Sau này, ông nhớ lại sở thích này hồi còn nhỏ đôi khi đã khiến ông phải gặp rắc rối như thế nào: "Những đứa trẻ lớn hơn làm ra mật mã, nhưng chỉ cần nắm được một vài từ thì thế nào tôi cũng tìm ra chìa khóa giải mã. Hậu quả của sự thông minh này thường là rất đau đớn: chủ nhân của những mật mã bị khám phá này đôi khi đã đón đánh tôi, mặc dù lỗi là ở chính sự ngu ngốc của họ". Những trận đòn này đã không làm Babbage nản lòng và ông vẫn tiếp tục bị thú giải mã lôi cuốn. Ông đã viết trong cuốn tự truyện của mình là "việc giải mã, theo tôi, là một trong những nghệ thuật hấp dẫn nhất".

Ông sớm có danh tiếng trong xã hội London với tư cách là một nhà phân tích mật mã, luôn sẵn sàng đương đầu mọi bức thư mã hóa và những người lạ đều có thể đến gặp ông với đủ mọi loại vấn đề rắc rối. Chẳng hạn, Babbage đã giúp đỡ một người viết tiểu sử đang tuyệt vọng tìm cách giải mã những ghi chú tốc ký của John Flamsteed, nhà thiên văn học Hoàng gia đầu tiên của Anh. Ông cũng đã giúp một nhà sử học giải được mật mã của Henrietta Maria, vợ của Charles I. Vào năm 1854, ông đã cộng tác với một luật sư và sử dụng phân tích mật mã để phát hiện ra một bằng chứng quan trọng trong một vụ án. Trong nhiều năm, ông đã tích lũy được một tập hồ sơ dày những thư từ mã hóa mà ông dự định sẽ sử dụng để viết một cuốn sách về phân tích mật

mã, với tựa đề *Triết lý giải mã*. Cuốn sách sẽ gồm hai ví dụ cho mỗi loại mật mã, một được giải mã để minh họa và một sẽ dùng làm bài tập cho người đọc. Không may, cũng giống như nhiều dự định lớn khác trong cuộc đời ông, cuốn sách này đã không bao giờ hoàn thành.

Trong khi hầu hết các nhà giải mã đều từ bỏ mọi hy vọng có thể giải được mật mã Vigenère, thì theo thư từ trao đổi với John Hall Brock Thwaites, một nha sĩ ở Bristol có cái nhìn khá ngây thơ về mật mã, Babbage lại rất có hứng thú thử giải mật mã đó. Năm 1854, Thwaites tuyên bố đã phát minh ra một loại mật mã mới mà thực tế thì nó tương tự với mật mã Vigenère. Ông đã viết cho *Tạp chí của Hội nghệ thuật* với ý định nhận bằng phát minh cho ý tưởng của mình, rõ ràng là không nhận thức được rằng ông đã bị muộn vài thế kỷ rồi. Babbage viết thư cho tờ tạp chí, chỉ ra rằng "mật mã này... là một dạng đã quá cũ rồi, và có thể tìm thấy ở rất nhiều cuốn sách". Thwaites không những không cảm thấy có lỗi mà còn thách đố Babbage giải được mật mã của ông ta. Việc có giải mã được hay không chẳng liên quan gì đến chuyện loại mật mã này có mới hay không, song sự tò mò của Babbage cũng đủ để khiến ông bắt tay vào việc tìm ra điểm yếu của mật mã Vigenère.

Giải một loại mật mã khó cũng chẳng khác gì trèo lên một bề mặt vách đá hoàn toàn dốc đứng. Các nhà giải mã tìm kiếm bất cứ một cái gờ hay vết nứt nào để có một lực đẩy dù là nhỏ nhất. Trong mật mã dùng một bảng chữ cái, họ bám vào tần suất của các chữ cái, vì những chữ cái thông dụng nhất, như **e**, **t**, và **a**, sẽ nổi bật lên bất kể chúng được che đậy bằng cách nào. Trong mật mã Vigenère dùng nhiều bảng chữ cái, tần suất cân bằng hơn rất

nhiều, vì người ta sử dụng khóa mã để chuyển đổi giữa các bảng chữ cái. Chính vì vậy, thoạt nhìn thì bề mặt vách đá dường như hoàn toàn trơn nhẵn.

Hãy nhớ rằng, sức mạnh lớn nhất của Vigenère đó là cùng một chữ cái sẽ được mã hóa bằng nhiều cách khác nhau. Chẳng hạn, nếu từ khóa là **KING** thì mỗi chữ cái trong bảng chữ cái thường có thể được mã hóa theo bốn cách khác nhau, vì từ khóa có bốn chữ cái. Mỗi chữ cái trong từ khóa xác định một bảng chữ cái riêng biệt trong hình vuông Vigenère, được trình bày ở Bảng 7. Cột **e** trong hình vuông được làm nổi rõ để thấy chữ cái **e** được mã hóa khác nhau như thế nào, tùy thuộc vào chữ cái nào trong từ khóa xác định sự mã hóa đó.

Nếu **K** trong **KING** được dùng để mã hóa chữ cái **e**, thì chữ cái tương ứng trong văn bản mật mã sẽ là **O.**

Nếu **I** trong **KING** được dùng để mã hóa chữ cái **e**, thì chữ cái tương ứng trong văn bản mật mã sẽ là **M.**

Nếu **N** trong **KING** được dùng để mã hóa chữ cái **e**, thì chữ cái tương ứng trong văn bản mật mã sẽ là **R.**

Nếu **G** trong **KING** được dùng để mã hóa chữ cái **e**, thì chữ cái tương ứng trong văn bản mật mã sẽ là **K**.

Tương tự, toàn bộ các từ cũng sẽ được mã hóa theo các cách khác nhau: ví dụ như từ **the** chẳng hạn, nó có thể được mã hóa thành **DPR**, **BUK**, hay **ZRM**, tùy thuộc vào vị trí của nó đối với từ khóa. Mặc dù điều đó làm cho việc giải mã trở nên khó khăn nhưng cũng không hẳn là không thể thực hiện được. Điểm quan trọng phải lưu ý là nếu chỉ có bốn cách để mã hóa từ **the** và trong bức thư gốc có một vài từ **the** thì chắc chắn là một số trong bốn

cách mã hóa đó sẽ được lặp lại trong văn bản mật mã. Ví dụ dưới đây sẽ minh họa cho điều này, với cụm từ **The Sun and the Man in the Moon** được mã hóa bằng mật mã Vigenère với từ khóa **KING** như sau.

Từ khóa
K I N G K I N G K I N G K I N G K I N G K I N G
Văn bản thường
t h e s u n a n d t h e m a n i n t h e m o o n
Văn bản mật mã
D P R Y E V N T N B U K W I A O X B U K W W B T

Từ **the** được mã hóa thành **DPR** trong trường hợp thứ nhất, và sau đó là **BUK** trong trường hợp thứ hai và thứ ba. Nguyên nhân của sự lặp lại nhóm **BUK** đó là từ **the** thứ hai ở vị trí cách từ **the** thứ ba tám chữ cái và 8 là bội số của số các chữ cái trong từ khóa, tức là 4. Nói cách khác, từ **the** thứ hai được mã hóa theo mối quan hệ của nó đối với từ khóa (**the** đứng ngay dưới **ING**), và đến từ **the** thứ ba thì từ khóa đã quay vòng đúng hai lần, lặp lại mối quan hệ đó và vì vậy mà lặp lại cách mã hóa.

Babbage đã nhận ra rằng kiểu lặp lại này đã giúp ông có được một chỗ đặt chân chính xác mà ông cần để chinh phục mật mã Vigenère. Ông đã có thể xác định được một chuỗi những bước đi tiếp tương đối là đơn giản mà bất kỳ nhà giải mã nào cũng có thể làm theo để giải loại *mật mã không thể phá nổi* cho đến lúc này. Để minh họa cho kỹ thuật tuyệt vời của ông, hãy tưởng tượng chúng ta bắt được một bản mật mã như trình bày ở Hình 13. Chúng ta biết rằng nó đã được mã hóa bằng mật mã Vigenère, song chúng ta không biết gì về văn bản gốc và từ khóa vẫn còn là một bí ẩn.

Bảng 7 Hình vuông Vigenère được sử dụng kết hợp với từ khóa **KING**. Từ khóa xác định bốn bảng mật mã riêng rẽ, nên chữ cái **e** có thể được mã hóa thành **O**, **M**, **R** hoặc **K**.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Bước đầu tiên trong cách giải mã của Babbage đó là tìm những dãy chữ cái xuất hiện hơn một lần trong văn bản mật mã. Sự lặp lại này có thể xuất hiện theo hai cách. Chắc chắn nhất là cùng một dãy các chữ cái trong văn bản gốc được mã hóa bằng cách

dùng cùng một nhóm chữ cái trong từ khóa. Cách thứ hai, ít gặp hơn, là hai dãy chữ cái khác nhau trong văn bản gốc được mã hóa bằng cách sử dụng các nhóm chữ cái khác nhau trong từ khóa, nhưng ngẫu nhiên lại dẫn tới dãy các chữ cái giống nhau trong văn bản mật mã. Nếu chúng ta hạn chế chỉ xét các dãy dài thì không cần tính đến khả năng thứ hai và trong trường hợp này, chúng ta sẽ chỉ để ý đến những dãy gồm bốn chữ cái trở lên. Bảng 8 thống kê những lần lặp lại như vậy và khoảng cách giữa mỗi lần lặp lại đó. Chẳng hạn dãy **E-F-I-Q** xuất hiện ở dòng đầu tiên trong bản mật mã và sau đó lặp lại ở dòng thứ 5, cách dãy đầu tiên 95 chữ cái.

Hình 13 Bản mật mã sử dụng mật mã Vigenère

Được sử dụng để mã hóa văn bản thường thành văn bản mật mã, từ khóa mã cũng được người nhận sử dụng để giải mã văn bản mật mã trở lại thành văn bản thường. Vì vậy, nếu chúng ta xác định được từ khóa thì việc giải mã là hoàn toàn dễ dàng. Đến lúc này, chúng ta chưa có đủ thông tin để tìm ra từ khóa, song Bảng 8 cung cấp cho chúng ta một số đầu mối rất tốt để tìm ra số chữ cái trong từ khóa. Ngoài việc liệt kê các dãy lặp lại và khoảng cách giữa mỗi lần lặp lại này, phần còn lại của bảng cho biết *các thừa số* - tức các ước số của khoảng cách. Chẳng hạn, dãy **W-C-X-Y-M** lặp lại sau 20 chữ cái và các số 1, 2, 4, 5, 10 và 20 là các thừa số, vì 20 chia hết cho chúng. Các thừa số này đặt ra sáu khả năng:

(1) Từ khóa gồm một chữ cái và được quay vòng 20 lần giữa các lần mã hóa.
(2) Khóa mã gồm hai chữ cái và được quay vòng 10 lần giữa các lần mã hóa
(3) Khóa mã gồm bốn chữ cái và được quay vòng 5 lần giữa các lần mã hóa
(4) Khóa mã gồm năm chữ cái và được quay vòng 4 lần giữa các lần mã hóa
(5) Khóa mã gồm mười chữ cái và được quay vòng 2 lần giữa các lần mã hóa
(6) Khóa mã gồm hai mươi chữ cái và được quay vòng 1 lần giữa các lần mã hóa.

Khả năng đầu tiên có thể loại vì từ khóa mà chỉ có một chữ cái thì sẽ trở thành mật mã dùng một bảng chữ cái - tức là chỉ dùng một dòng của mật mã Vigenère để mã hóa toàn bộ bản

mật mã, và bảng chữ cái mật mã là không thay đổi; chắc chắn là người lập mật mã sẽ không làm như vậy. Để chỉ một trong các khả năng, dấu ✓ được điền vào các cột thích hợp ở Bảng 8. Mỗi dấu ✓ chỉ một độ dài khả dĩ của từ khóa.

Bảng 8 Số lần lặp và các khoảng cách trong bản mật mã

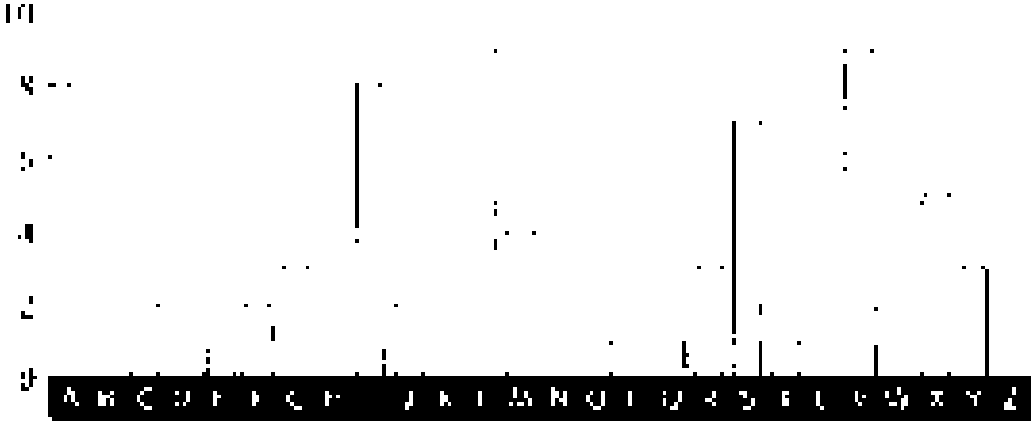
Chuỗi lặp	Khoảng cách lặp	Số chữ cái khả dĩ trong từ khóa (các thừa số)																		
F-F-I-Q					✓														✓	
P-S-D-L-P					✓															
W-C-X-Y-M		✓		✓	✓					✓										✓
E-T-R-L		✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

Để xác định độ dài của từ khóa là 2, 4, 5, 10 hay 20, chúng ta hãy nhìn vào các thừa số ở tất cả các khoảng cách. Vì từ khóa có vẻ như có 20 chữ cái hoặc ít hơn nên Bảng 8 liệt lê các thừa số từ 20 hoặc nhỏ hơn cho mỗi khoảng cách. Có một khuynh hướng khá rõ ràng, đó là khoảng cách chia hết cho 5. Và thực tế, tất cả các khoảng cách đều chia hết cho 5. Dãy lặp lại đầu tiên, **E-F-I-Q**, có thể được giải thích là từ khóa gồm năm chữ cái, được quay vòng 19 lần giữa lần mã hóa thứ nhất và thứ hai. Dãy thứ hai, **P-S-D-L-P**, có thể được giải thích là từ khóa gồm năm chữ cái và được quay vòng 1 lần giữa lần mã hóa thứ nhất và thứ hai. Dãy lặp lại thứ ba, **W-C-X-Y-M** với từ khóa gồm năm chữ cái và được quay vòng bốn lần giữa lần mã hóa thứ nhất và thứ hai. Dãy thứ tư, **E-T-R-L**, được giải thích với từ khóa gồm năm chữ cái và quay vòng 24 lần giữa lần mã hóa thứ nhất và thứ hai. Tóm lại, tất cả trước sau đều có chung từ khóa gồm năm chữ cái.

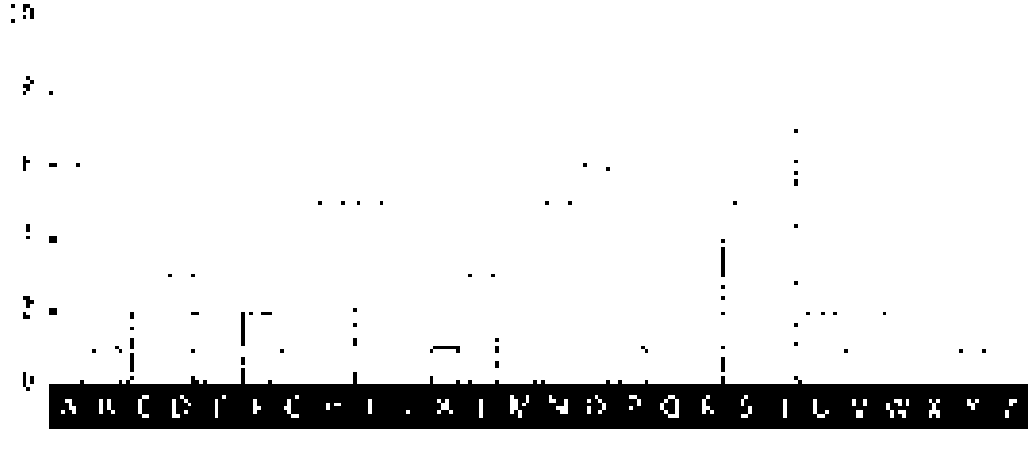
Giả sử từ khóa mã thực sự gồm có năm chữ cái, bước tiếp theo là tìm ra các chữ cái thực của từ khóa. Lúc này, chúng ta ký hiệu từ khóa mã là L1-L2-L3-L4-L5, trong đó L1 biểu thị chữ cái thứ nhất và cứ tiếp tục như vậy. Quá trình mã hóa sẽ bắt đầu với việc mã hóa chữ cái thứ nhất trong văn bản thường theo chữ cái thứ nhất trong từ khóa là L1. L1 xác định một dòng trong hình vuông Vigenère, nghĩa là cung cấp một bảng chữ cái mã dùng để thay thế cho chữ cái đầu tiên trong văn bản thường. Tuy nhiên, đến khi mã hóa chữ cái thứ hai, người mã hóa sẽ phải sử dụng L2 để xác định một dòng khác trong hình vuông Vigenère, tức là cung cấp một bảng chữ cái mã khác. Chữ cái thứ ba sẽ được mã hóa theo L3, chữ cái thứ tư theo L4 và thứ năm theo L5. Mỗi chữ cái trong từ khóa sẽ cung cấp một bảng chữ cái mật mã khác nhau cho việc mã hóa. Tuy nhiên, đến chữ cái thứ sáu trong văn bản thường sẽ quay trở lại mã hóa theo L1, chữ cái thứ bảy theo L2 và cứ tiếp tục vòng lặp như vậy. Nói cách khác, mật mã dùng nhiều bảng chữ cái ở đây gồm năm bảng chữ cái mật mã, mỗi bảng chịu trách nhiệm mã hóa 1/5 văn bản gốc và điều quan trọng nhất là chúng ta đã biết làm thế nào để giải mã đối với bảng mật mã dùng một bảng chữ cái.

Chúng ta tiếp tục các bước tiếp sau. Chúng ta biết rằng một trong số các dòng trong hình vuông Vigenère, được xác định bởi L1 cung cấp bảng chữ cái mật mã để mã hóa các chữ cái thứ 1, thứ 6, thứ 11, thứ 16,... trong văn bản gốc. Chính vì vậy, nếu nhìn vào các chữ cái thứ 1, thứ 6, thứ 11, thứ 16,... trong văn bản mật mã, chúng ta có thể sử dụng một phương pháp cũ là phân tích tần suất để tìm ra bảng chữ cái mật mã đang còn là ẩn số. Hình 14 cho thấy tần suất của từng chữ cái ở các vị trí thứ 1, thứ 6, thứ 11, thứ 16,... của văn bản mật mã, đó là các chữ cái W, I, R, E,... Đến

đây, chúng ta hãy nhớ rằng mỗi bảng chữ cái mật mã trong hình vuông Vigenère chỉ đơn giản là một bảng chữ cái chuẩn bị dịch đi một giá trị nằm trong khoảng từ 1 đến 26. Vì vậy, tần suất từng chữ cái trong Hình 14 cũng phải có đặc điểm tương đồng với tần suất của từng chữ cái trong bảng chữ cái chuẩn, ngoại trừ việc nó đã bị dịch chuyển đi một đoạn nào đó. Bằng cách so sánh phân bố (các chữ cái) theo L1 và phân bố chuẩn, có thể tìm ra khoảng dịch chuyển. Hình 15 cho thấy phân bố tần suất chuẩn cho một đoạn văn bản thường bằng tiếng Anh.



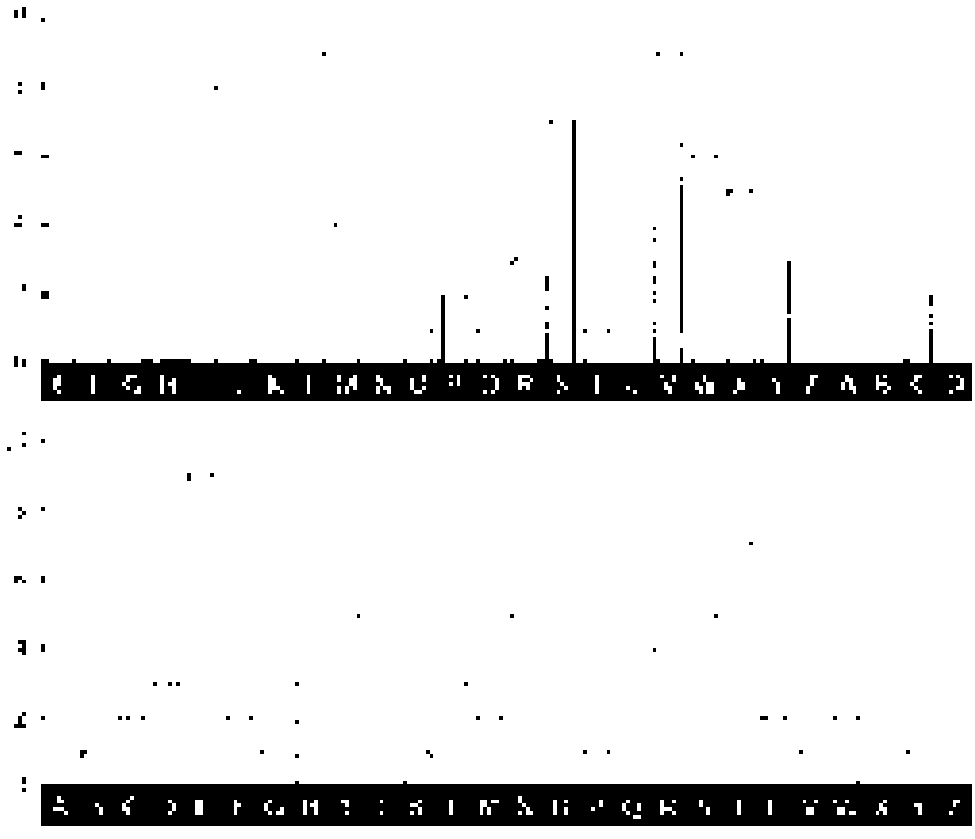
Hình 14 Phân bố tần suất của các chữ cái trong văn bản mật mã được mã hóa bằng cách sử dụng bảng chữ cái mật mã theo L_1 (số lần xuất hiện)



Hình 15 Phân bố tần suất chuẩn (số lần xuất hiện lấy cơ sở từ một đoạn văn bản thường có cùng số chữ cái với văn bản mật mã)

Phân bố chuẩn có các đỉnh, những đoạn bằng phẳng và các thung lũng và để làm khớp với phân bố mật mã theo L1, chúng ta hãy tìm tập hợp những đặc điểm nổi bật nhất. Chẳng hạn, trong phân bố chuẩn có ba cột tại **R-S-T** (Hình 15) và sau đó tụt xuống một đoạn dài về phía bên phải kéo dài qua 6 chữ cái từ **U** đến **Z** cùng nhau tạo nên một cặp đặc điểm rất khác biệt. Đặc điểm tương tự trong phân bố theo L1 chỉ có thể là ba cột tại **V-W-X** và sau đó tụt xuống một đoạn dài từ **Y** đến **D**. Điều này cho thấy tất cả các chữ cái mã hóa theo L1 đã dịch chuyển đi bốn vị trí, hay L1 xác định bảng mật mã bắt đầu từ **E, F, G, H**,... Điều này có nghĩa là chữ cái đầu tiên trong từ khóa, tức L1, có thể là chữ **E**. Giả thuyết này có thể kiểm chứng lại bằng cách dịch phân bố theo L1 lùi lại bốn chữ cái và so sánh nó với phân bố chuẩn. Hình 16 biểu diễn cả hai sự phân bố để tiện so sánh. Sự tương ứng giữa các đỉnh chính là rất rõ, điều này cho thấy sẽ là an toàn nếu cho rằng từ khóa thực sự bắt đầu bằng chữ **E**.

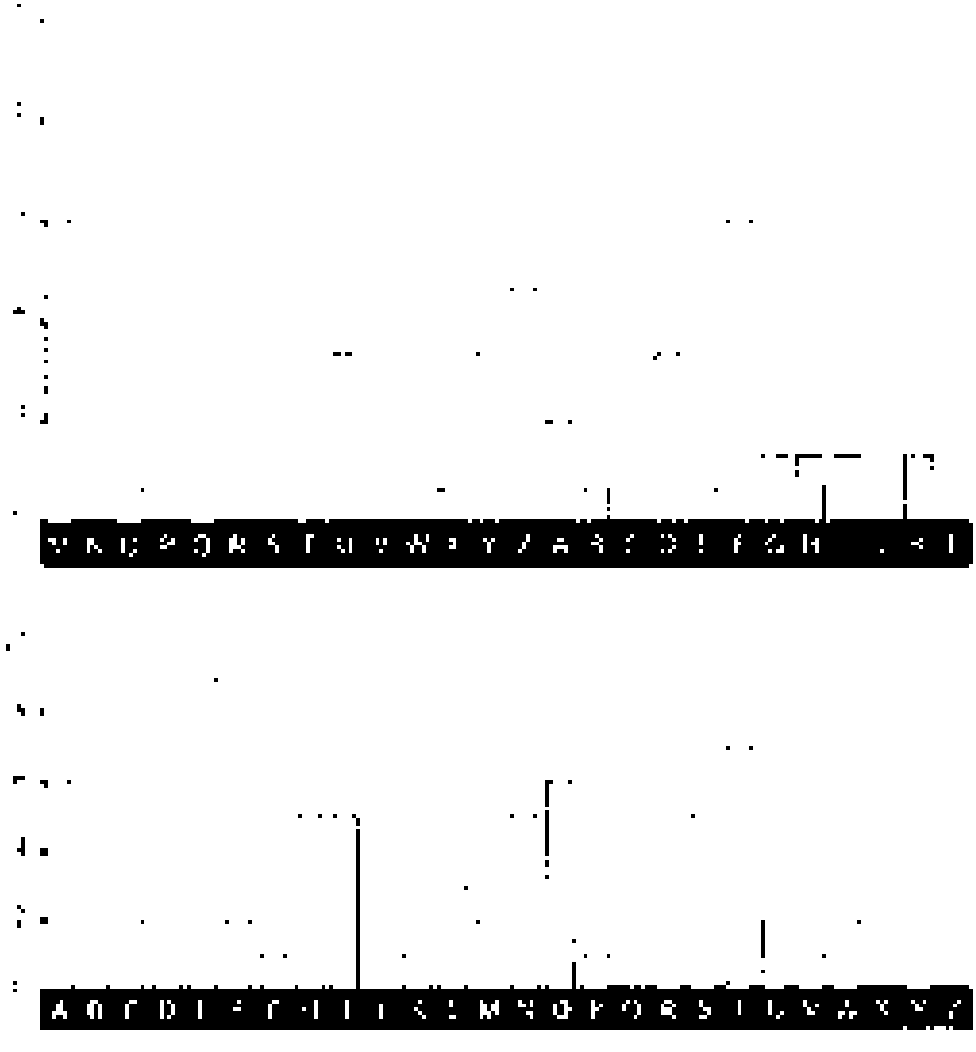
Tóm lại, việc tìm kiếm những chỗ lặp lại trong văn bản mật mã cho phép chúng ta xác định được độ dài của từ khóa, đó là 5, tức là gồm năm chữ cái. Điều này cho phép ta chia bản mật mã thành 5 phần, mỗi phần được mã hóa theo một bảng chữ cái xác định bởi mỗi chữ cái trong từ khóa. Bằng cách phân tích phân đoạn của văn bản mật mã được mã hóa theo chữ cái thứ nhất của từ khóa, chúng ta đã có thể biết được chữ cái này, tức L1, rất có thể là chữ **E**. Quá trình này được lặp lại để xác định chữ cái tiếp theo trong từ khóa. Phân bố tần suất được thiết lập cho các chữ cái thứ 2, thứ 7, thứ 12, thứ 17,... trong văn bản mật mã. Một lần nữa, phân bố này, trình bày ở Hình 17, lại được so sánh với phân bố chuẩn để xác định được khoảng dịch chuyển.



Hình 16. Phân bố theo L_1 được dịch lùi lại bốn chữ cái (hình bên trên) so với phân bố tần suất chuẩn (hình bên dưới). Tất cả các đỉnh và hõm chính đều ăn khớp nhau.

Hình 17 Phân bố tần suất đối với những chữ cái trong văn bản mật mã được mã hóa theo bảng chữ cái mật mã được xác định theo L_2 (số lần xuất hiện).

Phân bố lần này khó phân tích hơn một chút. Không có ba đỉnh liền nhau nào rõ ràng tương ứng với **R-S-T**. Tuy nhiên, sự tụt xuống kéo dài từ **G** đến **L** cũng rất khác biệt, và có thể nó tương ứng với sự tụt xuống mà ta có thể thấy từ **U** đến **Z** trong phân bố chuẩn. Nếu đúng như vậy thì chúng ta có thể hy vọng rằng ba đỉnh **R-S-T** xuất hiện tại **D-E-F** nhưng tại **E** lại không có đỉnh nào. Đến đây, chúng ta tạm bỏ qua cái đỉnh bị mất, coi như là một sự không đều về mặt thống kê, và trở lại cảm nhận ban đầu của chúng



Hình 18 Phân bố theo L_2 dịch lùi lại 12 vị trí (hình trên) được so sánh với phân bố tần suất chuẩn (hình dưới). Phần lớn các đỉnh và hõm chính đều ăn khớp nhau.

ta, đó là sự giảm dần từ G đến L là một đặc điểm bị dịch chuyển đáng chú ý. Điều này cho thấy tất cả các chữ cái được mã hóa theo L2 đã được dịch chuyển 12 vị trí, hay L2 xác định một bảng mật mã bắt đầu bằng **M, N, O, P**,... và chữ cái thứ hai của từ khóa, tức L2, là **M**. Một lần nữa, giả thuyết này có thể kiểm chứng lại bằng việc dịch lùi phân bố theo L2 đi 12 vị trí và so sánh nó với phân bố chuẩn. Hình 18 trình bày cả hai phân bố và sự tương ứng giữa các đỉnh chính là rất rõ. Điều này cho thấy đã an toàn để giả định rằng chữ cái thứ hai của từ khóa mã thực sự là **M**.

Tôi sẽ không tiếp tục phân tích nữa, chỉ cần nói rằng việc phân tích các chữ cái thứ 3, thứ 8, thứ 13,... sẽ giúp ta nhận được chữ cái thứ ba của từ khóa là **I**, phân tích chữ cái thứ 4, thứ 9, thứ 14,... sẽ cho chữ cái thứ tư là **L** và phân tích chữ cái thứ 5, thứ 10, thứ 15 sẽ cho chữ cái thứ năm của từ khóa là **Y**. Vậy từ khóa là **EMILY**. Giờ thì ta có thể đảo ngược mật mã Vigenère và hoàn tất việc giải mã. Chữ cái đầu tiên của văn bản mật mã là **W**, và nó được mã hóa theo chữ cái đầu tiên của từ khóa là **E**. Làm ngược lại, chúng ta hãy nhìn vào hình vuông Vigenère, và tìm chữ cái **W** ở dòng bắt đầu bằng chữ **E** và chúng ta tìm ra chữ cái ở đầu cột. Chữ cái này là **s**, đó chính là chữ cái đầu tiên của văn bản thường. Lặp lại quá trình này, chúng ta thấy văn bản thường bắt đầu bằng **sittheedownandhavenoshamecheekbyjowl**... Bằng việc thêm vào những dấu cách giữa các từ và dấu câu, cuối cùng chúng ta nhận được:

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?

Let me screw thee up a peg:
Let me loose thy tongue with wine:
Callest thou that thing a leg?
Which is thinnest? thine or mine?

Thou shalt not be saved by works:
Thou hast been a sinner too:
Ruined trunks on withered forks,
Empty scarecrows, I and you!

Fill the cup, and fill the can:
Have a rouse before the morn:
Every moment dies a man,
Every moment one is born.

Đây là một đoạn trong bài thơ *The Vision of Sin* của Alfred Tennyson. Từ khóa hóa ra lại là tên của vợ Tennyson, Emily Sellwood. Sở dĩ tôi chọn một đoạn trong bài thơ này để làm ví dụ minh họa cho việc giải mã là bởi vì nó gợi đến sự trao đổi thư từ khá kỳ lạ giữa Babbage và nhà thơ vĩ đại này. Là một nhà thống kê sắc sảo và cũng là người đã lập các bảng về tỷ lệ tử vong, nên Babbage cảm thấy bực bội với hai câu *"Every moment dies a man, Every moment one is born"* (Mỗi lúc có một người chết đi, Mỗi lúc lại có một người ra đời), đó chính là hai dòng cuối trong văn bản thường ở trên. Vì vậy, ông đã đề nghị sửa lại bài thơ "đẹp khác lạ" này của Tennyson:

> Thật rõ ràng là nếu điều này là đúng, thì dân số thế giới sẽ không thay đổi... Tôi xin đề nghị khi tái bản bài thơ này, ông nên viết lại là "Mỗi lúc một người chết đi, Mỗi lúc lại có $1^{1}/16$

người ra đời"... Con số chính xác dài quá không thể ghi trong một dòng được, nhưng tôi tin là con số 1[1]/16 là đủ chính xác cho thi ca rồi.
Trân trọng chào Ngài,
Charles Babbage.

Sự giải thành công mật mã Vigenère của Babbage có lẽ đạt được vào năm 1854, ngay sau xích mích của ông với Thwaites, song phát minh của ông hoàn toàn không được biết đến vì ông không bao giờ công bố nó. Phát minh này chỉ được biết đến vào thế kỷ 20, khi các học giả nghiên cứu một số lượng lớn những ghi chép của ông. Trong khi đó, kỹ thuật của ông cũng đã được khám phá một cách độc lập bởi Friedrich Wilheim Kasiski, một sĩ quan quân đội Phổ đã nghỉ hưu. Ngay từ năm 1863, khi ông này đã công bố đột phá giải mã của mình trong cuốn *Die Geheimschriften und die Dechiffrir-kunst* (Chữ viết bí mật và Nghệ thuật giải mã), kỹ thuật này đã được biết đến dưới cái tên Phép thử Kasiski, và đóng góp của Babbage hầu như không được biết đến.

Vậy tại sao Babbage lại không công bố việc hóa giải thành công một loại mật mã có tính chất sống còn như vậy? Chắc có lẽ ông vốn có thói quen không bao giờ kết thúc các dự án và không công bố những khám phá của mình, và đây cũng chỉ là một ví dụ nữa về thái độ không mấy dấn thân của ông. Tuy nhiên, cũng có một cách giải thích khác. Khám phá của ông xuất hiện ngay sau khi nổ ra Cuộc chiến tranh Crimê và có một thuyết cho rằng mật mã Vigenère là một lợi thế rõ ràng của người Anh trước kẻ thù người Nga của họ. Cũng có thể là Tình báo Anh đã yêu cầu Babbage giữ bí mật kết quả của ông, nhờ đó đã giúp họ đi trước phần còn lại của thế giới chín năm trời. Nếu đúng là như vậy thì

nó cũng phù hợp với truyền thống bưng bít những thành quả giải mã vì an ninh quốc gia đã tồn tại từ lâu, một tập quán vẫn còn tiếp tục trong thế kỷ 20.

Từ Cột nhắn tin đến Kho báu bí mật

Nhờ những tiến bộ của Charles Babbage và Friedrich Kasiski, mật mã Vigenère không còn an toàn nữa. Các nhà tạo mã không thể đảm bảo được sự an toàn nữa, và giờ thì các nhà giải mã đã thành công đoạt lại thế kiểm soát trong cuộc chiến thông tin liên lạc. Mặc dù các nhà tạo mã đã cố gắng thiết kế những dạng mật mã mới nhưng không có kết quả nào đáng kể trong suốt nửa sau của thế kỷ 19, và lĩnh vực mật mã chuyên nghiệp đã rơi vào tình trạng khá lộn xộn. Tuy nhiên, thời kỳ này cũng đã chứng kiến sự gia tăng cực lớn sự quan tâm của công chúng đối với mật mã.

Sự phát triển của máy điện báo đã từng gây ra sự quan tâm về mặt thương mại đối với khoa mật mã, giờ lại dấy lên sự quan tâm của công chúng đối với nó. Mọi người đã nhận ra sự cần thiết phải bảo vệ thư từ cá nhân vốn có bản chất nhạy cảm cao, và nếu cần thiết, họ sẵn sàng sử dụng mã hóa ngay cả khi phải mất thêm thời gian để gửi thư, và vì vậy điện phí cũng tăng. Nhân viên điện báo có thể gửi thư thường bằng tiếng Anh với tốc độ 35 từ một phút vì họ có thể nhớ toàn bộ các cụm từ và truyền chúng đi chỉ trong nháy mắt, trong khi với mớ lộn xộn các chữ cái tạo nên một văn bản mật mã thì việc truyền đi chậm hơn rất nhiều, vì nhân viên điện báo phải kiểm tra từng dãy chữ cái một. Tất nhiên, mật mã mà công chúng sử dụng không thể chống được

sự tấn công của các nhà giải mã chuyên nghiệp, song cũng đủ để bảo vệ trước con mắt của những kẻ rình mò.

Vì con người trở nên thoải mái hơn với mật mã, họ bắt đầu bộc lộ những kỹ năng về mật mã của mình theo nhiều cách khác nhau. Chẳng hạn, những đôi bạn trẻ yêu nhau ở nước Anh thời nữ hoàng Victoria thường bị cấm không được công khai bày tỏ tình yêu và không thể liên lạc bằng thư từ vì bố mẹ họ có thể bắt gặp và đọc được nội dung của nó. Điều này khiến họ phải gửi thư đã mã hóa cho nhau qua các cột nhắn tin trên báo. Những cột nhắn tin này đã gợi sự tò mò của những nhà giải mã, họ tìm những bức thư ngắn này và tìm cách giải mã những nội dung ướt át trong đó. Người ta đồn rằng Charles Babbage cũng say mê trò chơi này cùng với những người bạn của mình là Charles Wheatstone và Nam tước Lyon Playfair, họ đã cùng nhau phát triển *mật mã Playfair* khá tinh xảo (xem Phụ lục E). Có lần, Wheatstone giải mã một tin nhắn trên tờ *Times* của một sinh viên Oxford, định rủ người yêu trốn nhà để cùng nhau đi xây tổ ấm. Vài ngày sau, Wheatstone gửi đăng một bức thư, được mã hóa bằng cùng loại mật mã như của chàng sinh viên, khuyên đôi trẻ không nên nổi loạn và hành động nông nổi như vậy. Ngay sau đó, trên cột báo xuất hiện bức thứ thứ ba, lần này thì không mã hóa gì hết và là của cô gái: "Charlie, đừng viết nữa. Mật mã của mình đã bị lộ rồi".

Trong suốt thời kỳ này, có rất nhiều những đoạn tin mã hóa xuất hiện trên các báo. Các nhà tạo mã bắt đầu đưa những đoạn văn bản mật mã lên báo đơn giản chỉ là để thách đố các đồng nghiệp của mình. Trong một số trường hợp khác, thì những đoạn tin mã hóa lại được sử dụng để đả kích các tổ chức hoặc nhân vật của công chúng. Tờ *Times* có lần đã bất cẩn cho đăng một tin

được mã hóa: "*Times* là Jeffreys của giới báo chí". Tờ báo được ví như quan tòa Jeffreys, một nhân vật đầy tai tiếng ở thế kỷ 17, ý nói nó là một tờ báo nhẫn tâm và xấu xa, hành xử như một cái loa phát thanh của chính phủ.

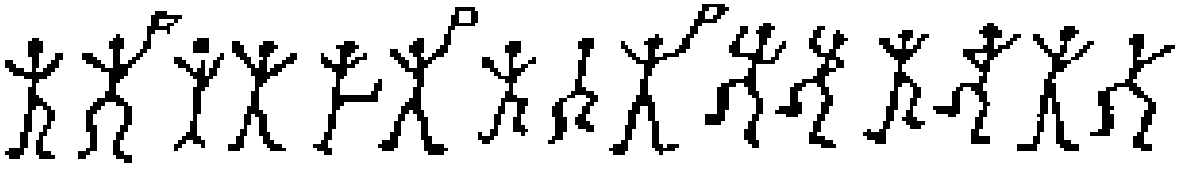
Một ví dụ khác về sự quen thuộc của công chúng với mật mã đó là sự sử dụng rộng rãi việc mã hóa bằng lỗ châm kim. Nhà viết sử người cổ Hy Lạp là Aeneas đã khuyến nghị chuyển thư tín bí mật bằng cách dùng kim châm những lỗ nhỏ dưới các chữ cái nhất định trong một trang văn bản, mà bề ngoài tưởng như là vô hại, nó nhìn giống như có một số chấm nhỏ dưới một số chữ cái trong đoạn văn mà bạn đang đọc. Nhưng xem kỹ ra, đây lại là lá thư bí mật mà người nhận định trước có thể đọc được dễ dàng. Tuy nhiên, nếu người ngoài nhìn thoáng qua, họ có thể không nhận thấy những lỗ châm kim và do đó không biết đó là một bức thư bí mật. Hai ngàn năm sau, những người Anh viết thư cũng đã sử dụng chính phương pháp này, không phải để bảo vệ bí mật mà là để tránh phải trả cước phí. Trước khi sử dụng hệ thống bưu phí vào giữa những năm 1800, gửi một bức thư đi cứ 100 dặm tốn một siling, vượt quá khả năng chi trả của hầu hết người dân. Tuy nhiên, báo chí thì lại được gửi miễn cước phí và điều này đã tạo khe hở cho những thần dân tằn tiện của nữ hoàng Victoria. Thay vì viết và gửi thư, người ta sử dụng lỗ châm kim để viết thư trên trang nhất của tờ báo. Sau đó họ gửi báo qua bưu điện mà không phải trả một xu nào.

Sự say mê ngày càng tăng của công chúng với kỹ thuật mã hóa cũng có nghĩa là chẳng bao lâu sau, mật mã đã tìm ra con đường đi vào văn học thế kỷ 19. Trong tiểu thuyết *Hành trình tới tâm Trái đất* của Jules Verne, văn bản mật mã là một cuộn da ghi chi

chít những mẫu tự *rune* (chữ Đức cổ) chỉ dẫn bước đầu tiên đi vào cuộc hành trình vĩ đại. Các ký tự này là bộ phận của một mã thay thế làm phát sinh ra một văn bản bằng tiếng Latin, nó chỉ có nghĩa khi các chữ cái đảo ngược lại: "Hỡi vị lữ khách táo bạo, hãy đi xuống miệng của núi lửa Sneffels khi bóng của ngọn núi Scartaris chạm tới nó trước ngày đầu tiên của tháng Bảy, từ đó bạn sẽ đi đến tâm của Trái đất". Vào năm 1885, Verne cũng đã sử dụng mật mã như là một yếu tố then chốt trong cuốn tiểu thuyết *Mathias Sandorff* của ông. Ở Anh, một trong những nhà văn giỏi nhất trong việc hư cấu về mật mã, đó là Ngài Arthur Conan Doyle. Và việc Sherlock Holmes là một chuyên gia trong lĩnh vực mật mã là điều không có gì phải ngạc nhiên và theo như ông ta giải thích với bác sĩ Watson thì (Holmes) là "tác giả của một cái chuyên khảo vặt vãnh về một chủ đề, mà trong đó, tôi đã phân tích một trăm sáu mươi loại mật mã khác nhau". Vụ giải mã nổi tiếng nhất của Holmes được kể trong truyện *Cuộc phiêu lưu của những hình nhân nhảy múa*, trong đó mật mã là những người hình que, mỗi tư thế biểu thị cho một chữ cái.

Ở phía bên kia bờ Đại Tây dương, Edgar Allan Poe cũng rất quan tâm đến phân tích mật mã. Là cây bút của tờ *Người đưa thư hàng tuần Alexander* ở Philadelphia, ông đã đưa ra một thách đố cho độc giả khi tuyên bố rằng ông có thể giải bất kỳ loại mật mã thay thế dùng một bảng chữ cái nào. Hàng trăm độc giả đã gửi đến những bản mật mã của họ và ông đã giải mã thành công tất cả số đó. Mặc dù điều này chẳng đòi hỏi gì nhiều ngoài việc phân tích tần suất, song độc giả của Poe cũng rất ấn tượng trước những thành quả của ông. Một fan hâm mộ đã coi ông "là một nhà giải mã tài năng và uyên thâm bậc nhất từ trước tới nay".

Năm 1843, hăng hái khai thác sự ham thích mà ông đã tạo nên, Poe đã viết một truyện ngắn về mật mã, được các nhà giải mã chuyên nghiệp khắp nơi công nhận là một tác phẩm văn học hư cấu hay nhất về đề tài này. *Con bọ bằng vàng* là một câu chuyện kể về William Legrand, người đã tìm thấy một con bọ lạ thường, một con bọ bằng vàng, và dùng một mẩu giấy nằm gần ngay cạnh để nhặt nó lên. Tối đó, anh phác thảo hình con bọ lên chính mẩu giấy đó rồi đưa lại gần ánh sáng ngọn lửa lò sưởi để xem mình vẽ có chính xác không. Tuy nhiên, hình phác thảo của anh bị mờ đi bởi một loại mực vô hình chợt hiện lên do hơi nóng của ngọn lửa. Legrand nghiên cứu những ký tự nổi trên mẩu giấy và hiểu rằng mình đã có trong tay một bản mật mã chỉ dẫn cách tìm kho báu của Thuyền trưởng Kidd. Phần còn lại của câu chuyện là một minh họa cổ điển cho phương pháp phân tích tần suất, kết quả giải mã là Legrand đã tìm được những manh mối do Thuyền trưởng Kidd để lại và tìm ra kho báu bí mật của ông ta.



Hình 19 Một đoạn văn bản mật mã trong cuốn *Cuộc phiêu lưu của những hình nhân nhảy múa* của Ngài Arthur Conan Doyle, một cuộc phiêu lưu của Sherlock Holmes

Mặc dù *Con bọ bằng vàng* hoàn toàn là hư cấu, song một câu chuyện có thật ở thế kỷ 19 cũng có những yếu tố tương tự. Đó là bản mật mã của Beale có liên quan đến những việc làm ăn đầy mạo hiểm ở miền Viễn Tây hoang dã của nước Mỹ. Một chàng cao bồi đã cóp nhặt được một kho của cải khổng lồ, một

kho báu bí mật trị giá 20 triệu đôla và một tập giấy tờ đã được mã hóa đầy bí ẩn mô tả vị trí cất giấu kho báu đó. Những gì chúng ta biết về câu chuyện này, kể cả những giấy tờ đã được mã hóa, có trong một cuốn sách nhỏ được xuất bản vào năm 1885. Mặc dù chỉ có 23 trang, song cuốn sách đã thách thức bao nhiêu thế hệ các nhà giải mã và cuốn hút hàng trăm người săn tìm kho báu.

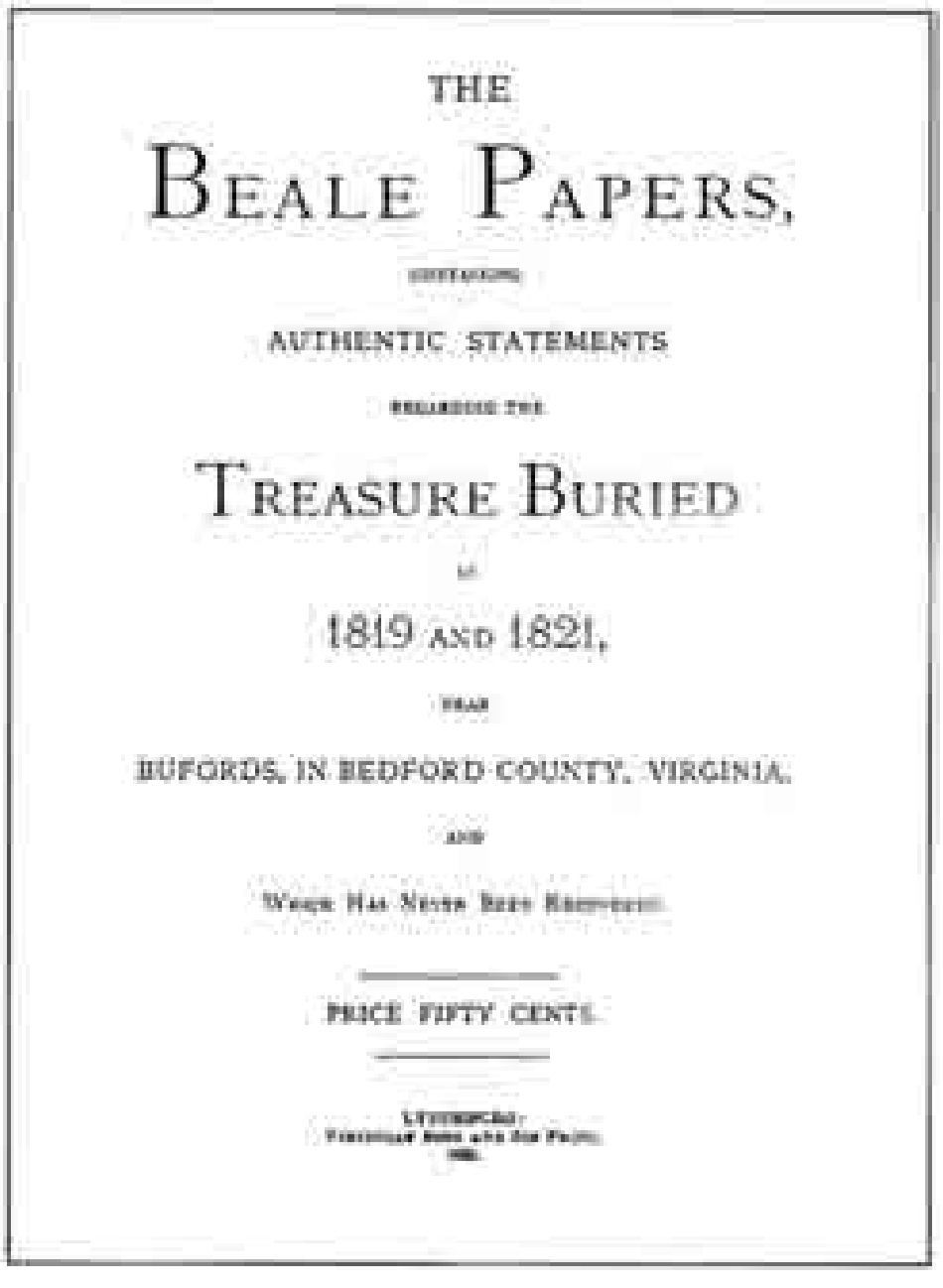
Câu chuyện bắt đầu ở khách sạn Washington ở Lynchburg, bang Virginia, sáu mươi lăm năm trước khi xuất bản cuốn sách nhỏ nói trên. Theo cuốn sách này thì khách sạn và người chủ của nó, Robert Morriss, đã được đánh giá rất cao: "tính tình tử tế, chân thật, nghiêm túc của ông, tài quản lý và cắt đặt công việc giỏi đã mau chóng khiến ông trở nên một ông chủ nổi tiếng và danh tiếng của ông lan truyền sang cả các bang khác. Khách sạn của ông là một ngôi nhà đặc biệt nhất trong thị trấn và chẳng có cuộc hội họp sang trọng nào lại không được tổ chức ở đó". Tháng Một năm 1820, một người lạ mặt có tên là Thomas J. Beale cưỡi ngựa đến Lynchburg và nghỉ tại khách sạn Washington. "Ông ta cao khoảng 1,8m", Morriss nhớ lại, "cặp mắt đen và mái tóc cùng màu, ăn mặc kiểu cổ hơn so với thời đó. Vóc dáng cân đối cho thấy ông ta là một người có sức mạnh và khả năng hoạt động phi thường; song có một đặc điểm hơi khác biệt là da mặt ông ta đen sạm, như thể bị phơi nắng quá nhiều và thời tiết đã làm cho da sạm lại và bạc màu, tuy nhiên điều đó cũng không hề làm giảm phong độ của ông, và tôi nghĩ ông ấy là người đàn ông đẹp nhất mà tôi đã từng gặp". Mặc dù Beale đã sống toàn bộ phần còn lại của mùa đông ở khách sạn của Morriss và "cực kỳ thân thiện với tất cả mọi người, đặc biệt là các quý bà", song

ông ta không bao giờ nói gì về thân thế của mình, gia đình hay mục đích chuyến đi của ông. Sau đó, đến cuối tháng Ba, ông ta rời khách sạn một cách đột ngột hệt như lúc đến.

Hai năm sau, tháng Một năm 1822, Beale trở lại khách sạn Washington, "da dẻ trông còn đen sạm hơn bao giờ hết". Một lần nữa, ông lại dành cả phần còn lại của mùa đông ở Lynchburg và lại biến mất vào mùa xuân, nhưng trước đó, ông đã tin cậy giao lại cho Morriss một chiếc hộp bằng sắt được khóa kín và nói trong đó có chứa "những giấy tờ có giá trị và rất quan trọng". Morriss cất chiếc hộp ở một nơi an toàn và không nghĩ gì đến nó nữa cho đến khi nhận được một lá thư của Beale, đề ngày 9 tháng Năm năm 1822, được gửi từ St. Louis. Sau vài lời đùa cợt và một đoạn nói về dự định đi đến vùng đồng cỏ "để săn bò rừng và đọ sức với gấu xám", lá thư của Beale đã tiết lộ tầm quan trọng của chiếc hộp:

> Nó đựng những giấy tờ rất quan trọng đối với tài sản của bản thân tôi cũng như rất nhiều người khác cùng làm ăn với tôi, và trong trường hợp tôi chết, thì sự biến mất của nó là không thể nào cứu vãn nổi. Vì vậy, chắc ông hiểu sự cần thiết phải bảo vệ nó thật thận trọng và cảnh giác ngăn chặn không cho thảm họa khủng khiếp đó xảy ra. Có thể không ai trong chúng tôi trở lại, nên ông làm ơn bảo vệ cẩn thận chiếc hộp này trong khoảng thời gian là 10 năm kể từ ngày ghi trên lá thư này, và nếu sau thời gian đó, tôi hoặc không ai được tôi ủy quyền đến đòi lại, thì ông hãy mở nó ra bằng cách phá khóa. Ông sẽ thấy ngoài các giấy tờ đề gửi ông, còn có một số giấy tờ khác mà ông không thể đọc được nếu không có chìa khóa. Chìa khóa đó tôi đã trao tận tay cho một người bạn ở đây, đã niêm phong

và để gửi ông, đồng thời được đảm bảo ông sẽ chưa thể nhận được nó cho tới tháng Sáu năm 1832. Bằng chìa khóa này, ông sẽ hiểu tất cả những gì ông được yêu cầu phải làm.



THE

BEALE PAPERS,

AUTHENTIC STATEMENTS

TREASURE BURIED

1819 AND 1821,

BUFORDS, IN BEDFORD COUNTY, VIRGINIA.

PRICE FIFTY CENTS.

Hình 20 Trang bìa của cuốn *Những giấy tờ của Beale*, cuốn sách nhỏ chứa trong nó tất cả những gì chúng ta biết về kho báu bí ẩn của Beale.

Moriss đã bảo vệ chiếc hộp một cách đầy trách nhiệm, chờ Beale quay trở lại lấy, song người đàn ông da sạm đen đầy bí ẩn ấy đã không bao giờ quay trở lại Lynchburg. Ông đã biến mất mà không một lời giải thích, và không bao giờ có ai còn trông thấy ông nữa. Mười năm sau, Moriss lẽ ra đã có thể theo chỉ dẫn của lá thư và mở hộp nhưng ông dường như vẫn lưỡng lự không muốn phá khóa. Lá thư của Beale có nhắc tới một bức thư khác sẽ được gửi tới cho Moriss vào tháng Sáu năm 1832 để giải thích cách giải mã những giấy tờ bên trong chiếc hộp. Tuy nhiên, bức thư đã không bao giờ đến và có lẽ vì vậy mà Moriss cảm thấy là sẽ chẳng ích lợi gì khi mở chiếc hộp nếu như ông không thể giải mã được những gì có bên trong nó. Cuối cùng, vào năm 1845, sự tò mò của Moriss đã chiến thắng và ông đã phá khóa. Trong chiếc hộp là ba tờ giấy với các ký tự đã được mã hóa và một bức thư Beale viết bằng tiếng Anh thông thường.

Bức thư tiết lộ sự thật về Beale, về chiếc hộp và bản mật mã. Nó giải thích rằng vào tháng Tư năm 1817, gần ba năm trước khi Beale lần đầu tiên gặp Moriss, Beale và hai mươi chín người khác đã tham gia một cuộc hành trình xuyên nước Mỹ. Sau khi đi qua những vùng đất săn bắn giàu có của vùng đồng cỏ Viễn Tây, họ đã đến Santa Fe, và sống cả mùa đông trong một "thị trấn Mehicô nhỏ". Tháng Ba, họ tiến lên phía bắc và bắt đầu lần theo dấu vết của một đàn bò rừng lớn, hạ gục được nhiều con suốt dọc đường. Sau đó, theo lời Beale, họ đã gặp may:

> Một ngày, trong khi theo dấu vết lũ bò, cả bọn hạ trại trong một khe núi nhỏ, chừng 250 đến 350 dặm về phía bắc của Santa Fe. Họ cột ngựa lại và khi đang chuẩn bị bữa tối, một người

trong bọn đã phát hiện ra bên trong khe nứt của các tảng đá có dấu hiệu của vàng. Sau khi đưa nó cho những người khác xem, được xác nhận đúng là vàng, và kết quả tự nhiên là tất cả đều cực kỳ phấn khích.

Tiếp đó bức thư giải thích Beale và bạn bè ông với sự giúp đỡ của một bộ lạc địa phương, đã khai thác cả vùng trong vòng 18 tháng sau đó, và họ đã kiếm được một lượng vàng rất lớn và bạc cũng được tìm thấy ở gần đó. Trong lúc ấy, họ thống nhất rằng của cải mà họ mới kiếm được cần phải được chuyển đến một nơi an toàn, và họ đã quyết định mang nó trở về chôn cất tại một địa điểm bí mật ở Virginia quê nhà. Năm 1820, Beale đến Lynchburg cùng với số vàng bạc kiếm được, và ông đã tìm được một nơi thích hợp để cất giấu nó. Đó cũng chính là dịp ông trú tại khách sạn Washington lần đầu tiên và làm quen với Moriss. Khi ra đi vào cuối mùa đông, Beale nhập bọn trở lại với bạn bè, họ vẫn tiếp tục khai thác trong suốt thời gian ông vắng mặt.

Sau đó 18 tháng nữa, Beale trở lại Lynchburg để bổ sung thêm vào kho báu của mình. Lần này còn có thêm một lý do nữa:

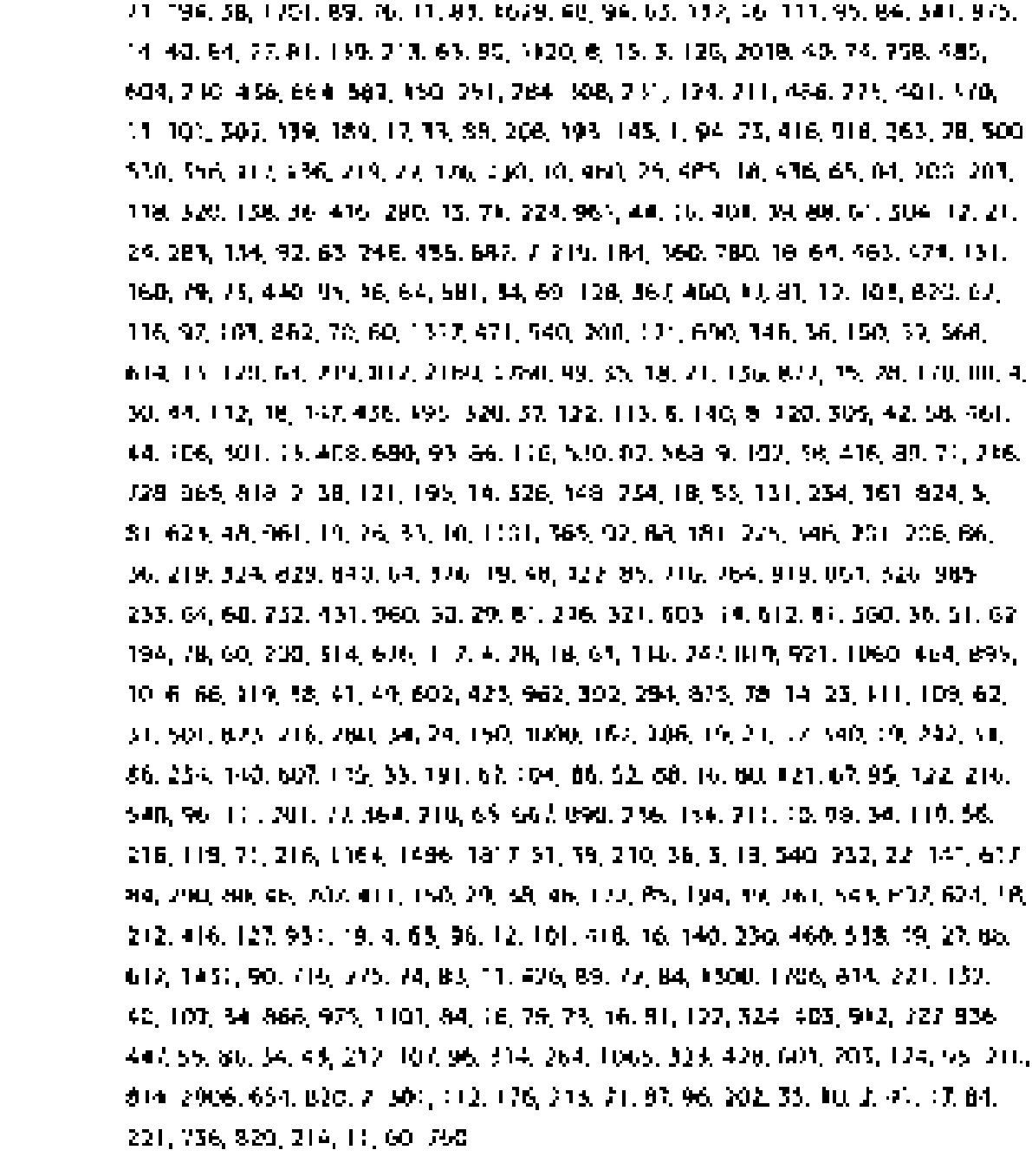
Trước khi tạm biệt bạn bè của mình ở vùng đồng cỏ, chúng tôi được khuyên là, nếu có tai nạn nào đó xảy ra với bản thân chúng tôi thì kho báu quá bí mật như vậy sẽ không thể đến với những người thân của mình nếu không trù tính trước cho những bất trắc như vậy. Vì vậy, tôi được giao lựa chọn một người nào đó thực sự đáng tin cậy, nếu tìm được và được cả nhóm chấp thuận, thì người đó sẽ được ủy thác thực hiện những ý nguyện của họ đối với phần của cải tương ứng của mỗi người.

Beale tin rằng Moriss là một người đàn ông liêm chính, chính vì vậy mà ông đã tin tưởng giao phó cho Moriss chiếc hộp có chứa ba tờ giấy đã được mã hóa mà ngày nay được gọi là bản mật mã của Beale. Mỗi tờ đều chứa hàng dãy các con số (được in lại ở các Hình 21, 22 và 23), và nếu giải mã được các con số này chắc sẽ tìm ra tất cả những chi tiết có liên quan; tờ giấy đầu tiên mô tả vị trí cất giấu kho báu, tờ giấy thứ hai liệt kê số lượng kho báu và tờ thứ ba là danh sách họ hàng của những người sẽ được nhận phần trong kho báu. Khi Moriss đọc được tất cả những điều này thì đã 23 năm trôi qua kể từ lần cuối cùng ông gặp Thomas Beale. Cho rằng Beale và bạn bè của ông đã chết, Moriss cảm thấy có trách nhiệm phải tìm ra kho vàng và chia nó cho họ hàng của họ. Tuy nhiên, không có chìa khóa mà Beale đã hứa, ông buộc phải giải mã từ con số không, một công việc đã khiến ông đau đầu trong suốt 20 năm sau, và cuối cùng thì ông đã thất bại.

Năm 1862, ở tuổi 84, Moriss biết rằng mình đã gần đất xa trời, và rằng ông phải chia sẻ bí mật về bản mật mã của Beale, nếu không thì mọi hy vọng thực hiện ý nguyện của Beale sẽ đi theo ông xuống mồ. Moriss giao phó việc đó cho một người bạn, song không may là thân thế của người này vẫn còn là một điều bí ẩn. Tất cả những gì chúng ta biết về người bạn của Moriss đó là ông ta chính là người đã viết cuốn sách nhỏ vào năm 1885, vì vậy sau đây, tôi sẽ gọi ông một cách đơn giản là *tác giả*. Tác giả lý giải lý do phải che giấu danh tính của mình trong cuốn sách nhỏ như sau:

> Tôi đoán trước rằng những giấy tờ này sẽ có một sức lan truyền rất lớn và để tránh bị tấn công bởi một số lượng thư từ khổng lồ đến từ khắp nơi trong Hợp chủng quốc, đặt ra đủ các loại

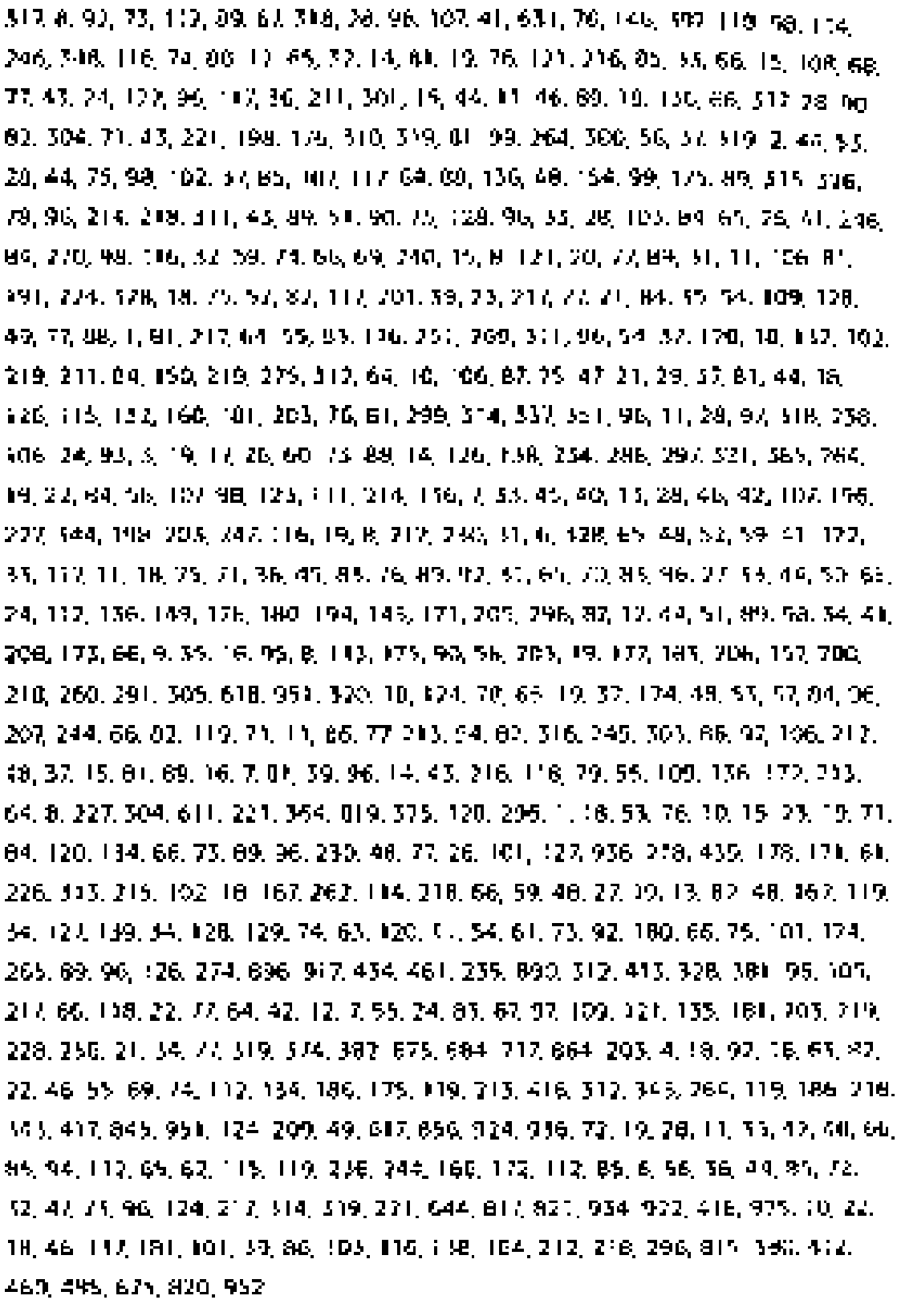
câu hỏi, và yêu cầu trả lời mà nếu định làm thì sẽ tốn toàn bộ thời gian của tôi, và chỉ làm thay đổi đặc tính công việc của tôi mà thôi, nên tôi đã quyết định không công bố danh tính, sau khi đảm bảo với tất cả những ai quan tâm rằng tôi đã nói ra tất cả những gì tôi biết và rằng tôi không hề thêm bớt một từ nào vào những nội dung trong cuốn sách này.



Hình 21 Bản mật mã thứ nhất của Beale

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 127, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 107, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 706, 398, 287, 63, 3, 6, 191, 122, 43,
254, 400, 106, 290, 314, 47, 48, 81, 96, 76, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 79, 125, 14, 20, 37, 105, 78,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 17, 131, 62, 115, 107, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 311, 2,
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 55, 106,
160, 113, 31, 107, 406, 230, 540, 320, 29, 66, 33, 201, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 65, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 63, 105, 807, 188, 96, 110, 16, 23, 33, 807, 150, 409, 408, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 403, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288

Hình 22 Bản mật mã thứ hai của Beale



Hình 23 Bản mật mã thứ ba của Beale

Để bảo vệ danh tính của mình, tác giả đã yêu cầu James B. Ward, một ủy viên đáng kính của hội đồng địa phương và là kiểm soát viên của hạt đường bộ làm đại diện và là người xuất bản cho mình.

Tất cả những gì chúng ta biết về câu chuyện lạ lùng về bản mật mã của Beale đều ở trong cuốn sách nhỏ này và chính nhờ tác giả mà chúng ta có được bản mật mã và những lời kể của Moriss về câu chuyện này. Thêm vào đó, tác giả cũng là người giải mã thành công bản mật mã thứ hai của Beale. Giống như bản mật mã thứ nhất và thứ ba, bản mật mã thứ hai cũng chỉ có một trang gồm toàn các con số, và tác giả đã giả định rằng mỗi số biểu thị cho một chữ cái. Tuy nhiên, số các con số lại vượt quá số các chữ cái trong bảng chữ cái, nên tác giả nhận ra rằng ông đang phải đương đầu với một loại mật mã, trong đó sử dụng một vài số để biểu thị cùng một chữ cái. Loại mật mã thỏa mãn tiêu chuẩn này được gọi là *mật mã sách (book cipher)*, trong đó một cuốn sách hoặc một đoạn văn bản bất kỳ nào đó chính là chìa khóa mã.

Đầu tiên, người mã hóa cần phải đánh số mỗi từ trong văn bản khóa mã (*key text*). Như vậy, mỗi số sẽ thay thế cho chữ cái đầu tiên của từ tương ứng. [1]For [2]example, [3]if [4]the [5]sender [6]and [7]receiver [8]agreed [9]that [10]this [11]sentence [12]were [13]to [14]be [15]the [16]keytext, [17]then [18]every [19]word [20]would [21]be [22]numerically [23]labeled, [24]each [25]number [26]providing [27]the [28]basis [29]for [30]encryption. (Ví dụ, nếu người gửi và người nhận thỏa thuận rằng câu này là văn bản khóa mã, thì mỗi từ sẽ được đánh số, mỗi số sẽ là cơ sở để mã hóa). Sau đó, thiết lập một bảng gắn mỗi số với chữ cái đầu tiên của từ tương ứng:

1	=	f	11	=	s	21	=	b
2	=	e	12	=	w	22	=	n
3	=	i	13	=	t	23	=	l
4	=	t	14	=	b	24	=	e
5	=	s	15	=	t	25	=	n
6	=	a	16	=	k	26	=	p
7	=	r	17	=	t	27	=	t

Một bức thư giờ đã có thể được mã hóa bằng cách thay thế các chữ cái trong văn bản thường bằng các con số theo bảng trên. Trong bảng này, chữ cái thường **f** sẽ được thay thế bằng số **1**, và chữ cái thường **e** được thay thế bằng các số **2**, **18**, **24** hoặc **30**. Vì văn bản khóa mã của chúng ta là một câu ngắn nên ta không có các số thay thế cho các chữ cái hiếm gặp, như **x** và **z**, song chúng ta có đủ các số thay thế để mã hóa từ **beale**, đó là **14-2-8-23-18**. Nếu người nhận có một bản của văn bản khóa mã thì việc giải mã là rất đơn giản. Tuy nhiên, nếu một bên thứ ba chỉ bắt được văn bản mật mã thì việc giải mã phụ thuộc vào chuyện có xác định được văn bản khóa mã hay không. Tác giả của cuốn sách nhỏ viết, "Với ý tưởng này, tôi đã thử kiểm tra với mọi cuốn sách mà tôi có thể kiếm được, bằng cách đánh số các chữ cái của nó và so sánh với các con số trong những bản viết tay của Beale; tuy nhiên, tất cả đều vô ích cho đến khi bản Tuyên ngôn Độc lập đã cho tôi đầu mối đối với một trong ba bản mật mã, và làm sống lại mọi hy vọng của tôi".

Bản Tuyên ngôn Độc lập được lấy làm văn bản khóa mã cho bản mật mã thứ hai của Beale, và bằng việc đánh số các từ trong bản Tuyên ngôn là có thể giải mã được nó. Hình 24 trình bày

trang đầu tiên của bản Tuyên ngôn Độc lập, cứ 10 từ được đánh số một lần để giúp người đọc hình dung việc giải mã diễn ra như thế nào. Hình 22 trình bày bản mật mã với số đầu tiên là **115**, và từ thứ 115 trong bản Tuyên ngôn là "instituted", như vậy số đầu tiên biểu thị chữ **i**. Số thứ hai trong bản mật mã là **73**, chữ cái thứ 73 trong Tuyên ngôn là "hold", nên số thứ hai biểu thị cho chữ **h**. Và đây là toàn bộ bản giải mã, được in trong cuốn sách nhỏ:

> Tôi đã để kho báu ở hạt Bedford, cách Buford khoảng 4 dặm, trong một cái hố hay hầm ở sâu dưới lòng đất khoảng 6 bộ, các điều khoản dưới đây, cùng thuộc về những người có tên trong tờ giấy số "3", gồm:
>
> Kho thứ nhất gồm 1014 pao vàng và 3812 pao bạc, được nhập kho vào tháng Mười một năm 1819. Kho thứ hai được làm vào tháng Mười hai năm 1281 bao gồm 1907 pao vàng và 1288 pao bạc; còn có cả đá quý đổi ra từ bạc ở St. Louis để vận chuyển cho an toàn, trị giá 13.000 đôla.
>
> Tất cả những của cải trên được để trong những thùng sắt, nắp đậy bằng sắt. Hầm được lát thô bằng đá và các thùng đựng đặt trên đá và thùng nọ đặt trên thùng kia. Tờ giấy số "1" mô tả chính xác vị trí của hầm nên tìm ra nó không có khó khăn gì.

Điều đáng lưu ý là có một số lỗi nhỏ trong bản mật mã. Chẳng hạn, bản giải mã có từ "4 dặm" (*four miles*), dựa vào từ thứ 95 trong bản Tuyên ngôn Độc lập bắt đầu bằng chữ *u*. Tuy nhiên, từ thứ 95 lại là từ "*in*alienable". Điều này có thể là do sự bất cẩn của Beale trong khi mã hóa, hoặc cũng có thể là do trong bản Tuyên ngôn mà Beale có, từ thứ 95 là "*un*alienable", có xuất hiện ở một số bản vào thời kỳ đầu thế kỷ 19. Dù thế nào thì việc giải

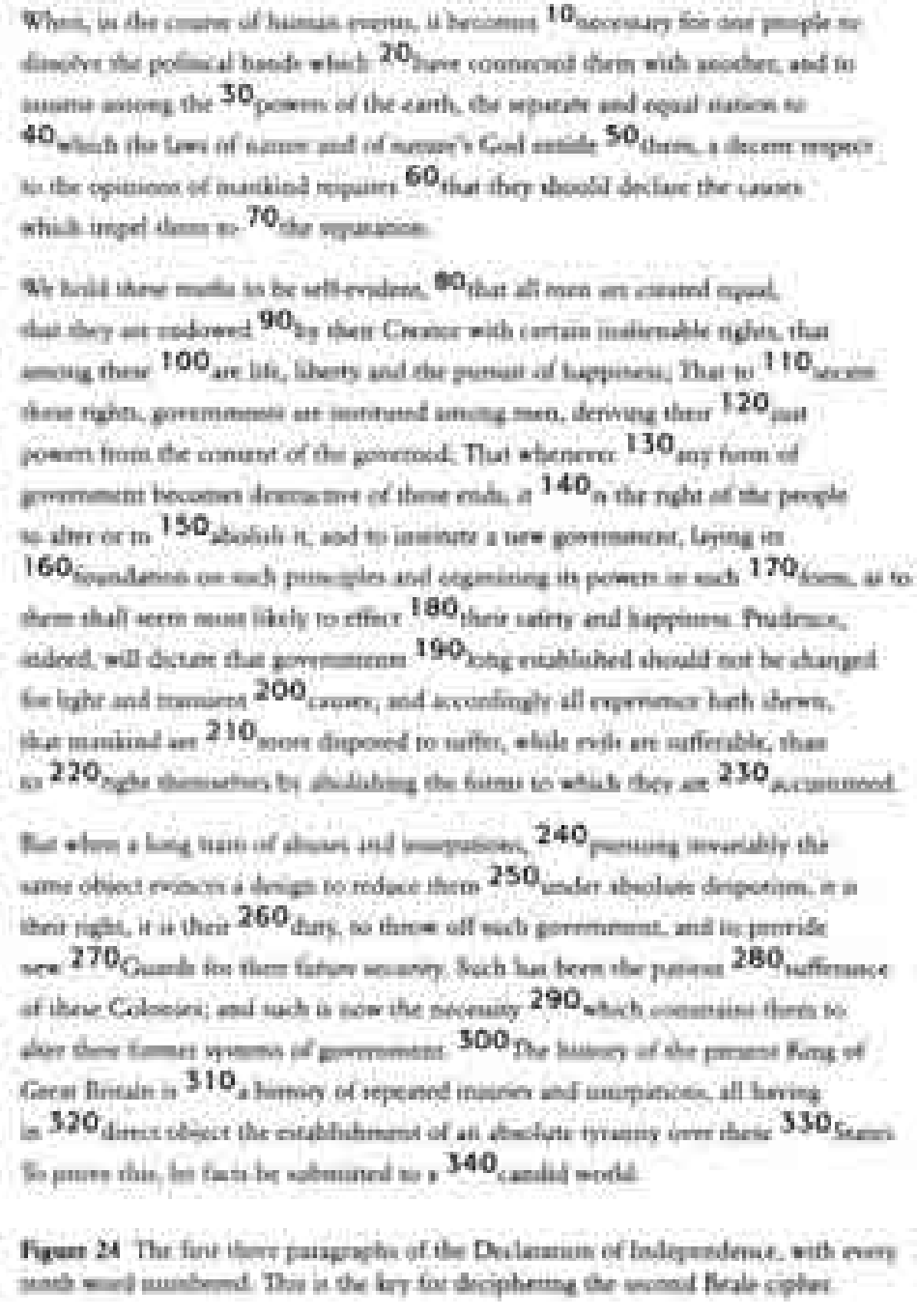
mã thành công này rõ ràng là đã cho thấy giá trị của kho báu - ít nhất là 20 triệu đôla tính theo giá vàng hiện nay.

Sẽ lại chẳng có gì đáng ngạc nhiên, một khi tác giả biết được giá trị của kho báu, ông càng dành nhiều thời gian để phân tích hai bản mật mã còn lại, đặc biệt là bản mật mã thứ nhất mô tả vị trí của kho báu. Tuy đã cố gắng không mệt mỏi, nhưng tác giả vẫn thất bại, và hai bản mật mã chẳng mang lại điều gì cho ông ngoài sự buồn phiền:

> Chính vì mất thời gian vào công việc nghiên cứu trên mà tôi bị sa sút từ chỗ đang giàu có sung túc đến cảnh bần hàn, làm cho những người mà tôi có trách nhiệm bảo vệ phải đau khổ, bất chấp sự phản đối của họ. Cuối cùng thì tôi cũng phải mở mắt ra trước cảnh sống khốn khó của họ và tôi đã quyết định ngay lập tức và vĩnh viễn cắt đứt mọi liên hệ với câu chuyện này và chuộc lại những sai lầm của mình, nếu có thể. Để làm được điều đó, cách tốt nhất là tránh thật xa sự cuốn hút của nó, vì vậy tôi quyết định công bố rộng rãi toàn bộ câu chuyện, và cất được gánh nặng trách nhiệm với ông Moriss.

Chính vì vậy, các bản mật mã này cùng với mọi chi tiết của câu chuyện mà tác giả biết đã được công bố vào năm 1885. Mặc dù một lần hỏa hoạn đã đốt cháy hầu hết các cuốn sách trong kho, song những quyển còn nguyên vẹn đã gây náo động ở Lynchburg. Trong số những kẻ săn tìm kho báu hăng hái nhất bị quyến rũ bởi bản mật mã của Beale có anh em nhà Hart, George và Clayton. Trong nhiều năm, họ đã nghiên cứu hai bản mật mã còn lại, sử dụng nhiều cách giải mã khác nhau, và có lúc họ tưởng như là mình đã tìm ra lời giải. Một cách giải mã sai đôi khi cũng có thể

dẫn đến một số từ đúng trong một biển các từ vô nghĩa, điều này đã khuyến khích người giải mã tạo ra đủ thứ cảnh báo để bào chữa cho những từ vô nghĩa đó. Đối với một người quan sát vô tư thì bản mật mã này chỉ là điều mơ ước chứ ngoài ra chẳng có



When, in the course of human events, it becomes 10necessary for one people to
dissolve the political bands which 20have connected them with another, and to
assume among the 30powers of the earth, the separate and equal station to
40which the laws of nature and of nature's God entitle 50them, a decent respect
to the opinions of mankind requires 60that they should declare the causes
which impel them to 70the separation.

We hold these truths to be self-evident, 80that all men are created equal,
that they are endowed 90by their Creator with certain inalienable rights, that
among these 100are life, liberty and the pursuit of happiness. That to 110secure
these rights, governments are instituted among men, deriving their 120just
powers from the consent of the governed. That whenever 130any form of
government becomes destructive of these ends, it 140is the right of the people
to alter or to 150abolish it, and to institute a new government, laying its
160foundation on such principles and organizing its powers in such 170form, as to
them shall seem most likely to effect 180their safety and happiness. Prudence,
indeed, will dictate that governments 190long established should not be changed
for light and transient 200causes; and accordingly all experience hath shewn,
that mankind are 210more disposed to suffer, while evils are sufferable, than
to 220right themselves by abolishing the forms to which they are 230accustomed.

But when a long train of abuses and usurpations, 240pursuing invariably the
same object evinces a design to reduce them 250under absolute despotism, it is
their right, it is their 260duty, to throw off such government, and to provide
new 270Guards for their future security. Such has been the patient 280sufferance
of these Colonies; and such is now the necessity 290which constrains them to
alter their former systems of government. 300The history of the present King of
Great Britain is 310a history of repeated injuries and usurpations, all having
in 320direct object the establishment of an absolute tyranny over these 330States.
To prove this, let facts be submitted to a 340candid world.

Figure 24 The first three paragraphs of the Declaration of Independence, with every tenth word numbered. This is the key for deciphering the second Beale cipher.

Hình 24 Ba đoạn đầu trong bản Tuyên ngôn Độc lập, được đánh số 10 từ một. Đây chính là chìa khóa để giải bản mật mã thứ hai của Beale.

ý nghĩa gì cả, song với một kẻ săn tìm kho báu mê muội thì nó lại hoàn toàn có nghĩa. Một trong những bản giải mã thử nghiệm của Hart đã xúi giục họ dùng chất nổ để khai quật một địa điểm; nhưng khốn thay, cái hố đào được đó chẳng có vàng bạc gì. Mặc dù Clayton Hart đã bỏ cuộc vào năm 1912 nhưng George vẫn tiếp tục cho đến năm 1952. Còn một fan cuồng nhiệt nữa của Beale là Hiram Herbert, Jr.. Người này lần đầu tiên quan tâm đến chuyện này vào năm 1923 và sự ám ảnh của ông ta còn kéo dài cho đến tận những năm 1970. Nhưng những cố gắng của ông cũng không có kết quả gì.

Các nhà giải mã chuyên nghiệp cũng tham gia vào cuộc truy tìm kho báu của Beale. Herbert O. Yardley, người sáng lập ra Văn phòng Mật mã U.S (ngày nay là Phòng Đen của Mỹ) vào cuối Thế chiến Thứ nhất, cũng bị bản mật mã Beale cuốn hút giống như đại tá William Friedman, một nhân vật quan trọng bậc nhất trong lĩnh vực giải mã của Mỹ trong suốt nửa đầu thế kỷ 20. Khi còn phụ trách Lực lượng Tình báo Tín hiệu, Friedman đã sử dụng bản mật mã của Beale như là một phần trong chương trình huấn luyện, chủ yếu là vì, như vợ ông kể, ông tin rằng mật mã này có "sự sáng tạo ma quỷ, được thiết kế đặc biệt để mê hoặc những người đọc thiếu cảnh giác". Kho lưu trữ Friedman, được lập ra sau cái chết của ông vào năm 1969 tại Trung tâm Nghiên cứu George C. Marshall, thường được các nhà sử học quân sự tới tham khảo, song phần lớn các vị khách lại là những người hâm mộ Beale, với hy vọng học hỏi được một vài chỉ dẫn của người đàn ông vĩ đại này. Gần đây hơn, một trong những nhân vật quan trọng trong cuộc săn tìm kho báu của Beale là Carl Hammer, giám đốc tin học của Sperry Univac đã nghỉ hưu và một trong những người đi

tiên phong trong việc giải mã bằng máy tính. Theo Hammer, "bản mật mã của Beale đã lôi cuốn ít nhất là 10% những bộ óc phân tích mật mã giỏi nhất trên cả nước. Nhưng không một chút nào trong những nỗ lực đó phải hối tiếc. Việc làm này - dù là những phương hướng dẫn tới ngõ cụt - đã được đền đáp một cách xứng đáng bằng cách làm cho khoa học máy tính phát triển và ngày càng tinh diệu". Hammer là thành viên sáng lập của Hiệp hội Kho báu và Mật mã Beale, được thành lập trong những năm 1960 để khuyến khích sự quan tâm đến câu chuyện đầy bí ẩn này. Ban đầu, Hiệp hội yêu cầu bất kỳ thành viên nào khám phá ra kho báu đều phải chia sẻ nó với các thành viên khác, nhưng nghĩa vụ này xem ra đã hạn chế rất nhiều người đi tìm kho báu Beale tham gia và vì vậy mà Hiệp hội đã bỏ đi điều kiện này.

Mặc cho những nỗ lực kết hợp của Hiệp hội, của những người săn tìm kho báu nghiệp dư lẫn những nhà giải mã chuyên nghiệp, bản mật mã thứ nhất và thứ ba của Beale vẫn còn là một bí ẩn trong suốt một thế kỷ, và vàng, bạc, đá quý vẫn chưa thấy tăm hơi đâu. Rất nhiều cố gắng giải mã xoay quanh bản Tuyên ngôn Độc lập, là chìa khóa để giải mã thành công bản mật mã thứ hai. Tuy việc đánh số một cách đơn giản các từ trong bản Tuyên ngôn không mang lại điều gì hữu ích cho bản mật mã thứ nhất và thứ ba, song các nhà giải mã vẫn thử các phương cách khác nhau, chẳng hạn như đánh số từ dưới lên hoặc đánh số xen kẽ, song đến nay vẫn không có kết quả. Một vấn đề là bản mật mã thứ nhất có một con số rất lớn là số **2906**, trong khi đó bản Tuyên ngôn chỉ có 1.322 từ. Các cuốn sách và văn bản khác cũng được xem như là những chìa khóa mã tiềm năng, và rất nhiều nhà giải mã cũng đã nghĩ đến khả năng về một hệ thống mã hóa hoàn toàn khác.

Bạn có thể ngạc nhiên trước sức mạnh không thể phá nổi của mật mã Beale, đặc biệt là khi nhớ rằng trước lúc chúng ta tạm rời cuộc chiến triền miên giữa các nhà tạo mã và giải mã thì các nhà giải mã đang ở thế thượng phong. Babbage và Kasiski đã tìm ra cách hóa giải mật mã Vigenère, và các nhà tạo mã đang phải vật lộn để tìm kiếm một loại mật mã khác thay thế cho nó. Vậy bằng cách nào mà Beale lại có thể gây ra được chuyện động trời đến như vậy? Câu trả lời là các bản mật mã của Beale đã được tạo ra trong hoàn cảnh đã đem lại một lợi thế rất to lớn cho các nhà tạo mã. Việc này chỉ liên quan đến ba bức thư và vì chúng gắn với một kho báu có giá trị đến như vậy nên Beale có thể đã chuẩn bị một văn bản chìa khóa đặc biệt cho bản mật mã thứ nhất và thứ ba. Thực tế, nếu văn bản chìa khóa được chính Beale sáng tác ra, thì điều này có thể giải thích vì sao việc nghiên cứu những tác phẩm đã xuất bản không thể phát hiện ra nó. Chúng ta có thể tưởng tượng rằng Beale đã tự viết một bài tiểu luận gồm 2.000 từ về chủ đề săn bò rừng mà chỉ có một bản duy nhất. Chỉ người nào có trong tay bài tiểu luận đó, tức bản chìa khóa duy nhất, mới có thể giải được bản mật mã thứ nhất và thứ ba của Beale. Chính Beale đã nói rằng ông ta đã đưa chìa khóa mã "tận tay một người bạn" ở St. Louis, song nếu người bạn đó đã đánh mất hoặc hủy chìa khóa mã đó thì các nhà giải mã có thể sẽ không bao giờ hóa giải được các bản mật mã của Beale.

Tạo ra một văn bản chìa khóa mã cho một bức thư thì an toàn hơn nhiều so với việc sử dụng chìa khóa là một cuốn sách đã xuất bản, song điều đó có ý nghĩa thực tế chỉ nếu người gửi có thời gian để tạo ra văn bản chìa khóa và chuyển nó cho người nhận đã định. Đó là những yêu cầu không khả thi đối với những liên

lạc có tính thường nhật. Trong trường hợp của Beale, ông ta có thể đã sáng tác ra văn bản chìa khóa vào những lúc rỗi rãi, rồi chuyển nó cho người bạn ông ở St. Louis bất cứ khi nào ông tình cờ đi ngang qua và sau đó nó được gửi qua bưu điện vào một thời điểm thích hợp trong tương lai, khi kho báu cần được thu hồi.

Một thuyết khác giải thích về sức mạnh không thể phá nổi của Beale đó là tác giả cuốn sách đã thay đổi chúng một cách có cân nhắc trước khi cho xuất bản. Có lẽ tác giả chỉ muốn buộc chìa khóa mã, mà rõ ràng là nó đang ở trong tay người bạn của Beale ở St. Louis, phải lộ diện. Nếu ông xuất bản chính xác bản mật mã thì người bạn đó có thể giải được mã, rồi đi chiếm đoạt kho vàng, và những nỗ lực của tác giả sẽ chẳng được đền đáp gì. Tuy nhiên, nếu bản mật mã bị thay đổi đi thì người bạn đó cuối cùng cũng sẽ nhận ra rằng ông ta phải cần đến sự giúp đỡ của tác giả và sẽ liên lạc với nhà xuất bản Ward và người này sẽ thông báo cho tác giả. Tác giả sau đó có thể trao bản mật mã chính xác để đổi lấy một phần của kho báu.

Cũng có thể kho báu đã được tìm thấy từ rất nhiều năm trước, và người khám phá ra nó đã lấy mang đi mà không bị người dân địa phương bắt gặp. Những người mê Beale theo trường phái âm mưu thì cho rằng Cơ quan An ninh Quốc gia (NSA) đã tìm thấy kho báu. Các cơ quan mật mã của Chính phủ trung ương của Mỹ có thể sử dụng những máy tính mạnh nhất cùng với một số bộ não xuất sắc nhất thế giới, họ có thể đã khám phá ra điều gì đó về những bản mật mã mà tất cả những người khác không thể vượt qua. Việc không công bố có lẽ là để giữ gìn danh tiếng tối mật của NSA - có người cho rằng NSA không phải là chữ viết tắt của Cơ quan An ninh Quốc gia mà là của *Never Say Anything*

(Không bao giờ nói gì) hoặc *No Such Agency* (Không có cơ quan nào như vậy).

Cuối cùng, chúng ta không thể loại trừ khả năng các bản mật mã của Beale chỉ là một trò lừa đảo tinh vi, và rằng Beale chưa bao giờ tồn tại. Những người hoài nghi thì cho rằng tác giả ẩn danh này, lấy cảm hứng từ cuốn *Con bọ bằng vàng* của Poe, đã hư cấu nên toàn bộ câu chuyện và xuất bản cuốn sách để kiếm lợi từ lòng tham của những người khác. Những người ủng hộ cho thuyết này đã tìm thấy những sơ hở và sự không thống nhất trong câu chuyện về Beale. Chẳng hạn, theo cuốn sách thì bức thư của Beale được để trong hộp sắt và được cho là viết vào năm 1822, có chứa từ "stampede" (sự chạy tán loạn), song từ này mãi đến năm 1834 mới được thấy xuất hiện trên các bản in. Tuy nhiên, cũng hoàn toàn có thể là từ này đã rất thông dụng ở miền Viễn Tây hoang dã trước đó rất nhiều và Beale có thể đã học được từ này trong những chuyến chu du của mình.

Một trong số những người không tin đầu tiên đó là nhà tạo mã Louis Kruh, người tuyên bố đã tìm thấy bằng chứng chứng tỏ tác giả cuốn sách cũng chính là người đã viết các bức thư của Beale, bức thư được cho là gửi từ St. Louis và bức trong chiếc hộp sắt. Ông đã tiến hành phân tích từ ngữ trong nguyên bản do tác giả viết và từ ngữ do Beale viết để tìm sự tương đồng giữa chúng. Kruh đã so sánh các tiêu chí như tỷ lệ các câu bắt đầu bằng từ "The", "Of" và "And", và số dấu phảy và dấu chấm phẩy trung bình trong mỗi câu, và cách viết - như việc sử dụng câu phủ định, bị động phủ định, động từ nguyên thể, mệnh đề quan hệ, v.v... Ngoài từ ngữ của tác giả và các bức thư của Beale, ông cũng phân tích bài viết của ba người Virginia khác ở thế kỷ 19.

Trong số năm bài viết đó thì bài viết của tác giả và của Beale gần như tương tự nhau, cho thấy chúng có thể được viết bởi cùng một người. Nói cách khác, điều đó cho thấy tác giả đã làm giả các bức thư của Beale và bịa ra toàn bộ câu chuyện.

Trong khi đó, nhiều nguồn khác lại chứng tỏ bản mật mã của Beale là có thực. Thứ nhất, nếu các bản mật mã không thể phá được này là trò lừa bịp thì có thể suy ra rằng kẻ lừa bịp đó lựa chọn các con số ít hoặc không có gì đáng lưu ý. Tuy nhiên, các con số ở đây lại tạo ra các hình mẫu phức tạp khác nhau. Một trong các hình mẫu này có thể tìm thấy bằng cách sử dụng chìa khóa mã là bản Tuyên ngôn Độc lập để giải bản mật mã thứ nhất. Nó không mang lại một từ nào có nghĩa mà chỉ là một dãy các chữ cái như **abfdefghiijklmmnohpp**. Mặc dù đây không phải là một danh sách các chữ cái hoàn chỉnh, song chắc chắn không phải là ngẫu nhiên. James Gillogly thuộc Hiệp hội Mật mã Mỹ không tin rằng bản mật mã của Beale là xác thực. Tuy nhiên, theo đánh giá của ông thì xác suất để dãy này xuất hiện một cách tình cờ chỉ nhỏ hơn một phần trăm triệu triệu, điều này cho thấy trong bản mật mã thứ nhất có tồn tại một nguyên tắc mã hóa nhất định. Có một thuyết cho rằng bản Tuyên ngôn thực sự là chìa khóa mã, song bản mã hóa đó lại được mã hóa một lần nữa; nói cách khác, bản mật mã thứ nhất của Beale được mã hóa bằng một quá trình hai bước, hay còn gọi là siêu mã hóa. Nếu đúng như vậy thì dãy chữ cái này có thể đã được sắp đặt như là một dấu hiệu khích lệ, một sự gợi ý rằng bước mã hóa đầu tiên đã được hoàn tất thành công.

Một bằng chứng nữa ủng hộ cho tính chân thực của những bản mật mã Beale đến từ việc nghiên cứu lịch sử. Có thể sử dụng

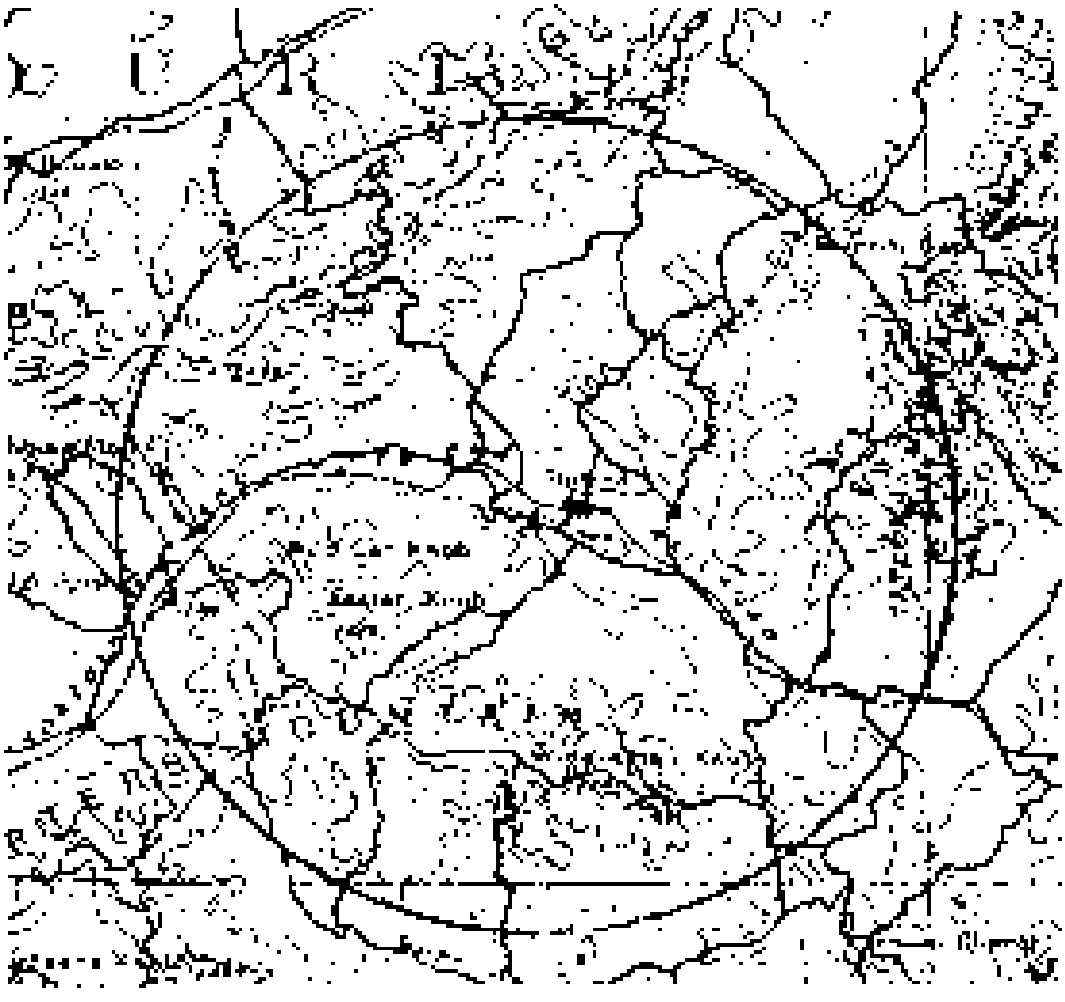
những nghiên cứu này để kiểm chứng câu chuyện về Thomas Beale. Peter Viemeister, một nhà sử học địa phương, đã thu thập và cho in rất nhiều nghiên cứu trong cuốn *Kho báu của Beale - Lịch sử một bí ẩn*. Viemeister bắt đầu bằng việc đặt câu hỏi liệu có bằng chứng nào chứng tỏ Thomas Beale thực sự tồn tại hay không. Sử dụng tài liệu về điều tra dân số năm 1790 và các tài liệu khác, Viemeister đã xác định được có vài Thomas Beale sinh tại Virginia và có nhân thân thích hợp với những chi tiết đã biết. Viemeister cũng đã thử kiểm tra những chi tiết khác trong cuốn *Các giấy tờ của Beale...*, chẳng hạn như hành trình của Beale đến Santa Fe và việc ông khám phá ra vàng. Chẳng hạn, một truyền thuyết của người Cheyenne (một bộ lạc da đỏ) vào khoảng năm 1820 có kể về vàng và bạc được lấy từ miền Viễn Tây và được giấu trong rặng Núi phía Đông. Hơn nữa, trong danh sách lưu của bưu cục vào năm 1820 ở St. Louis có cái tên "Thomas Beall", điều này cũng phù hợp với tuyên bố trong cuốn sách nói rằng Beale đã từng đi qua thành phố này vào năm 1820 trong chuyến trở lại miền Viễn Tây sau khi rời Lynchburg. Cuốn sách cũng nói rằng Beale đã gửi một lá thư từ St. Louis vào năm 1822.

Như vậy, câu chuyện về các bản mật mã của Beale dường như là có cơ sở, và vì vậy nó vẫn tiếp tục lôi cuốn các nhà giải mã và những kẻ săn tìm kho báu, như Joseph Jancik, Marilyn Parsons và con chó Muffin của họ. Vào tháng Hai năm 1983, họ đã bị phạt vì tội "xâm phạm một lăng mộ", sau khi bị bắt gặp đang đào bới bên trong nghĩa trang của Nhà thờ Mountain View vào lúc nửa đêm. Chẳng phát hiện được gì ngoài một chiếc quan tài, họ đã phải sống nốt phần còn lại của kỳ nghỉ cuối tuần trong nhà tù của hạt và cuối cùng là bị phạt 500 đôla. Những kẻ đào mộ

nghiệp dư này còn có thể tự an ủi mình khi biết rằng Mel Fisher, một người săn tìm kho báu chuyên nghiệp, đã từng kiếm được 40 triệu đôla vàng từ chiếc thuyền chiến *Nuestra Seíora de Atocha* bị đắm của Tây Ban Nha mà ông đã tìm ra ở Key West, Florida vào năm 1985, cũng chẳng khá hơn họ là mấy. Tháng Mười một năm 1989, Fisher nhận được thông tin từ một chuyên gia về Beale ở Florida, nói rằng kho báu của Beale được giấu ở Nhà máy xay Graham thuộc hạt Budford, Virginia. Được ủng hộ bởi một nhóm các nhà đầu tư giàu có, Fisher đã mua một mảnh đất dưới cái tên Mr. Voda để tránh gây sự chú ý. Sau một thời gian dài đào bới, ông đã không tìm được gì.

Một số kẻ săn kho báu đã từ bỏ hy vọng hóa giải được hai bản mật mã còn lại và thay vào đó, họ tập trung tìm đầu mối từ bản mật mã đã được giải mã. Chẳng hạn, cùng với việc mô tả giá trị của kho báu, bức mật mã còn chỉ ra rằng nó được cất giấu ở nơi "cách Buford chừng 4 dặm", địa danh này có lẽ muốn nói là thị trấn Buford, hoặc cụ thể hơn, là Quán trọ Buford, nằm ở trung tâm của tấm bản đồ trên Hình 25. Bức mật mã cũng nói rằng "hầm được lát thô bằng đá", nên rất nhiều người đã tìm kiếm dọc theo Nhánh sông Goose, một nguồn cung cấp đá tảng rất dồi dào. Mùa hè nào khu vực này cũng thu hút những người tràn trề hy vọng, một số được trang bị các máy dò kim loại, số khác đi cùng với những nhà chiêm tinh hay những nhà ngoại cảm. Gần thị trấn Budford có rất nhiều cửa hàng cho thuê dụng cụ, kể cả các máy đào công nghiệp. Nông dân địa phương thì lại không mấy niềm nở với những vị khách không mời này, vì họ thường xâm phạm đất đai, phá hoại hàng rào và đào những cái hố lớn.

Sau khi đọc xong câu chuyện về các bản mật mã của Beale, biết đâu có thể chính bạn cũng nảy ra ham muốn theo đuổi thách thức này cũng nên. Sự cám dỗ của một loại mật mã chưa thể phá nổi của thế kỷ 19 cộng với một kho báu trị giá 20 triệu đôla thật khó mà cưỡng lại được. Tuy nhiên, trước khi bạn khởi hành truy tìm kho báu, hãy lưu ý đến lời khuyên của tác giả cuốn sách nhỏ:



Hình 25 Một phần bản đồ Khảo sát Địa chất Mỹ năm 1891. Vòng tròn bán kính 4 dặm với tâm là Quán trọ Buford, vị trí mà bức mật mã thứ hai đã nói tới.

Trước khi công bố câu chuyện này, tôi xin có một vài lời nói với những ai có thể sẽ quan tâm tới nó, và đưa ra một lời khuyên nhỏ đúc rút từ những kinh nghiệm cay đắng của bản thân. Đó là, chỉ nên cống hiến khoảng thời gian có thể dành ra từ công việc chính đáng của mình cho công việc này, còn nếu không thể dành được chút thời gian nào thì đừng dính dáng gì đến nó... Một lần nữa, đừng bao giờ, như tôi đã làm, hy sinh cả bản thân mình và sự quan tâm đến gia đình mình cho một thứ mà có thể chỉ là ảo ảnh; nhưng, như tôi đã nói, khi công việc một ngày của bạn đã xong và bạn ngồi thoải mái bên lò sưởi ấm áp, thì dành một chút thời gian để suy nghĩ đến nó cũng chẳng hại gì và biết đâu có thể bạn sẽ được đền đáp.

3

Cơ giới hóa việc giữ bí mật

Vào cuối thế kỷ 19, khoa học mật mã thực sự ở trong tình trạng rối loạn. Kể từ khi Babbage và Kasiski phá vỡ sự an toàn của mật mã Vigenère, các nhà tạo mã vẫn đang tìm kiếm một loại mật mã mới, có thể thiết lập lại thông tin liên lạc bí mật, nhờ đó các doanh nhân và quân đội có thể tận dụng được tính tức thời của máy điện báo mà không sợ thông tin của mình bị đánh cắp và giải mã. Hơn nữa, vào lúc chuyển giao giữa hai thế kỷ, nhà vật lý người Italia Guglielmo Marconi đã phát minh ra một hình thái viễn thông còn mạnh hơn, khiến cho nhu cầu về mã hóa an toàn ngày càng trở nên cấp bách.

Năm 1894, Marconi bắt đầu thí nghiệm với một tính chất rất lạ của các mạch điện. Dưới những điều kiện nhất định, nếu một mạch điện có dòng điện đi qua, nó có thể tạo ra dòng điện cảm ứng ở một mạch điện cô lập khác ở cách xa nó. Bằng việc cải tiến thiết kế hai mạch điện, làm tăng thêm công suất và bổ sung thêm ăngten, Marconi đã mau chóng truyền và nhận tín hiệu qua khoảng cách tới 2,5 km. Vậy là ông đã phát minh ra sóng

vô tuyến (sóng radio). Máy điện báo đã được thiết lập trong nửa thế kỷ, song vẫn đòi hỏi phải có dây dẫn để truyền tín hiệu giữa người gửi và người nhận. Hệ thống của Marconi có một lợi thế cực lớn đó là không dây - tín hiệu truyền đi trong không khí như có phép lạ.

Năm 1896, để tìm kiếm hỗ trợ tài chính cho ý tưởng của mình, Marconi đã đến nước Anh, nơi ông đã nộp đơn xin bằng phát minh đầu tiên của mình. Để tiếp tục thí nghiệm, ông đã tăng phạm vi liên lạc vô tuyến, đầu tiên là truyền thông tin đi 15 km qua vịnh Bristol, và sau đó là 53 km qua eo biển English Channel giữa Anh và Pháp. Đồng thời, ông cũng bắt đầu tìm kiếm những ứng dụng có tính chất thương mại cho phát minh của mình, ông đã chỉ cho những nhà tài trợ tiềm năng thấy hai lợi thế chủ yếu của sóng vô tuyến: không đòi hỏi phải xây dựng những đường dây điện báo đắt tiền và có khả năng gửi thông tin giữa hai vị trí hoàn toàn cô lập với nhau. Ông đã tận dụng cơ hội quảng cáo tuyệt vời vào năm 1899, khi trang bị máy vô tuyến cho hai chiếc tàu giúp cho các nhà báo tham dự America Cúp, một giải đua thuyền buồm lớn nhất thế giới, có thể gửi bài về New York cho bản tin ngày hôm sau.

Sự quan tâm lại càng tăng thêm khi Marconi đã bác bỏ những ý kiến cho rằng liên lạc vô tuyến bị giới hạn bởi đường chân trời. Phe chỉ trích thì cho rằng sóng vô tuyến không bị uốn cong và lượn theo mặt cong của Trái đất nên liên lạc vô tuyến sẽ có giới hạn chỉ trong khoảng vài trăm km mà thôi. Marconi đã dự định chứng minh ý kiến phê phán của họ là sai bằng cách gửi một thông báo từ Poldhu ở Cornwall (tây nam nước Anh) tới Newfoundland (đông Canada) ở St. John, với khoảng cách là 3.500

km. Tháng Mười hai năm 1901, trong vòng 3 giờ mỗi ngày, người ta liên tục truyền đi chữ **S** (chấm-chấm-chấm) từ Poldhu, trong khi Marconi đứng trên vách đá lộng gió ở Newfoundland để dò bắt sóng vô tuyến. Ngày lại ngày, ông cố thả một cái diều khổng lồ lên cao hơn cốt cũng để nâng ăngten lên cao hơn. Chỉ ngay sau giữa trưa ngày 12 tháng Mười hai, Marconi đã dò bắt được ba dấu chấm yếu ớt, bức thư đầu tiên vượt qua Đại Tây dương. Thành công của Marconi là một điều bí ẩn và chỉ được giải thích vào năm 1924, khi các nhà vật lý khám phá ra tầng điện ly, một lớp khí quyển với ranh giới thấp nhất của nó cách mặt đất khoảng 60 km. Tầng điện ly đóng vai trò như một tấm gương phản xạ các sóng vô tuyến. Sóng vô tuyến cũng phản xạ từ bề mặt Trái đất nên các tín hiệu vô tuyến có thể đến bất cứ đâu trên thế giới sau một chuỗi các phản xạ giữa tầng điện ly và bề mặt Trái đất.

Phát minh của Marconi như trêu ngươi quân đội, những người nhìn nó với một cảm giác lẫn lộn vừa thèm muốn vừa lo lắng. Lợi thế chiến thuật của sóng vô tuyến đã quá rõ ràng: nó cho phép liên lạc trực tiếp giữa hai điểm bất kỳ mà không cần dây nối giữa chúng. Việc đặt đường dây như vậy thường là phi thực tế, đôi khi không thể thực hiện được. Trước kia, một viên chỉ huy hải quân trên cảng không thể liên lạc với tàu của mình, nó có thể bặt vô âm tín hàng tháng liên tục, nhưng sóng vô tuyến sẽ giúp anh ta điều phối cả một hạm đội bất kể các tàu đang ở đâu. Tương tự, sóng vô tuyến cũng giúp cho các tướng lĩnh chỉ huy các chiến dịch, giữ liên lạc liên tục với các tiểu đoàn mà không phụ thuộc vào sự di chuyển của họ. Sở dĩ tất cả các điều này đều có thể thực hiện được là nhờ bản chất của sóng vô tuyến, nó phát ra theo mọi hướng và đến được người nhận dù ở bất kỳ đâu. Tuy nhiên,

tính chất lan truyền rộng khắp này của sóng vô tuyến cũng lại là điểm yếu nhất của nó trong quân sự, bởi vì thông tin cũng sẽ đến tay kẻ thù như đến tay người nhận định trước. Do vậy, một sự mã hóa đáng tin cậy là rất cần thiết. Nếu kẻ thù có thể dò bắt được mọi tín hiệu vô tuyến thì các nhà tạo mã phải tìm ra một phương cách ngăn chặn việc giải mã các tín hiệu này.

Cảm giác pha trộn về sóng vô tuyến - vừa dễ liên lạc vừa dễ bị dò bắt - càng nổi lên rõ ràng hơn khi Thế chiến Thứ nhất bùng nổ. Tất cả các bên đều muốn tận dụng sức mạnh của sóng vô tuyến, nhưng lại không biết làm thế nào để bảo đảm an toàn. Cả phát minh về sóng vô tuyến lẫn cuộc Đại chiến đều làm tăng nhu cầu phải có một thứ mật mã hiệu quả. Người ta hy vọng sẽ có một đột phá, một loại mật mã mới, có thể thiết lập lại bí mật cho các sĩ quan quân đội. Tuy nhiên, từ năm 1914 đến 1918, không có một khám phá lớn nào, đơn giản chỉ là một chuỗi những thất bại trong việc tạo mã. Thực ra, các nhà tạo mã cũng có tạo ra được một số mật mã mới song chúng đều lần lượt bị phá vỡ.

Một trong những mật mã nổi tiếng nhất trong thời kỳ chiến tranh đó là *mật mã ADFGVX* của người Đức, được trình làng vào ngày 5 tháng Ba năm 1918, ngay trước một cuộc tấn công chủ yếu của quân Đức bắt đầu vào ngày 21 tháng Ba. Giống như mọi cuộc tấn công khác, cuộc công kích của quân Đức cũng dựa vào yếu tố bất ngờ để giành chiến thắng, và trong nhiều loại mật mã khác nhau, một hội đồng các nhà tạo mã đã lựa chọn mật mã ADFGVX, vì tin rằng nó có độ an toàn cao nhất. Thực tế, họ đã rất tự tin cho rằng mật mã này không thể hóa giải được. Sức mạnh của mật mã này nằm ở chính bản chất phức tạp của nó, ở đây có sự pha trộn giữa mã thay thế và mã chuyển vị (xem Phụ lục F).

Đến đầu tháng Sáu năm 1918, pháo binh của quân Đức chỉ còn cách Paris 100 km và đang chuẩn bị cho đòn quyết định cuối cùng. Chỉ còn hy vọng duy nhất cho quân Đồng minh là phải giải được mật mã ADFGVX để phát hiện chính xác nơi mà quân Đức dự định sẽ chọc thủng tuyến phòng ngự của họ. Thật may mắn là họ đã có một vũ khí bí mật, đó là một nhà giải mã có tên là Georges Painvin. Người đàn ông Pháp mảnh dẻ, da sẫm màu với trí tuệ sắc sảo này đã nhận ra khả năng của mình trước những vấn đề mật mã hóc búa chỉ sau cuộc gặp tình cờ với một thành viên của Phòng mật mã khi chiến tranh vừa nổ ra. Sau đó, tài năng vô giá của ông đã được tận dụng để xác định những điểm yếu trong mật mã của người Đức. Ông đã xoay xở ngày đêm với mật mã ADFGVX, mà vì nó ông đã bị sụt mất 15 kg.

Cuối cùng, đêm ngày mồng 2 tháng Sáu, ông đã giải được một bức thư mã hóa bằng ADFGVX. Sau thành công của Painvin, hàng loạt các bức thư khác đã được giải mã, trong đó có bức thư mang mệnh lệnh "Vận chuyển ngay đạn dược đến. Kể cả ban ngày nếu không bị phát hiện". Dòng bên trên bức thư cho biết nó được gửi từ một nơi nào đó nằm giữa Montdidier và Compiègne, cách Paris khoảng 80 km về phía bắc. Nhu cầu đạn dược khẩn cấp như vậy cho thấy nơi đó có thể là vị trí mà cuộc tấn công của quân Đức sắp xảy ra. Trinh sát trên không cũng xác nhận điều này là đúng. Lính Đồng minh đã được chuyển tới để tăng cường cho mặt trận này và một tuần sau, cuộc tấn công của quân Đức bắt đầu. Vì đã bị mất đi yếu tố bất ngờ, quân đội Đức đã bị đánh lui trong một trận chiến cực kỳ ác liệt kéo dài 5 ngày.

Việc phá được mật mã ADFGVX có thể coi là hiện tượng tiêu biểu của khoa mật mã trong suốt Thế chiến Thứ nhất. Mặc

dù đây là một loại mật mã mới khá mạnh, song chúng cũng chỉ là một dạng biến thể hoặc tổ hợp của các loại mật mã đã bị hóa giải ở thế kỷ 19. Tuy một số loại mật mã đó ban đầu đã mang lại sự an toàn, song cũng chẳng được lâu vì các nhà giải mã đều lần lượt phá được hết. Vấn đề lớn nhất của các nhà giải mã đó là phải xử lý một dung lượng thông tin liên lạc khổng lồ. Trước khi phát minh ra sóng vô tuyến, các bức thư chặn bắt được là những của quý hiếm và các nhà giải mã chỉ phải xử lý từng cái một. Tuy nhiên, trong Thế chiến Thứ nhất, số lượng thông tin liên lạc bằng sóng vô tuyến là cực kỳ lớn, và cứ mỗi một bức thư chặn bắt được lại tạo ra một luồng các văn bản mật mã ổn định mà các nhà giải mã phải xử lý. Người ta ước tính rằng quân Pháp đã chặn bắt được hàng trăm triệu từ qua thông tin liên lạc của quân Đức trong suốt cuộc Đại chiến.

Trong số những nhà giải mã thuộc thời kỳ chiến tranh thì người Pháp là có hiệu quả nhất. Khi bước vào cuộc chiến, họ đã là một đội ngũ giải mã mạnh nhất châu Âu, hậu quả của sự thất bại nhục nhã của quân Pháp trong cuộc chiến tranh giữa Pháp và Phổ. Napoleon III, với mong muốn phục hồi lại uy tín đang tàn tạ, đã xâm lược nước Phổ vào năm 1870, song ông đã không lường trước được sự liên minh giữa quân Phổ ở phía Bắc và các bang của Đức ở phía Nam. Dưới sự chỉ huy của Otto von Bismarck, quân Phổ đã nghiền nát quân Pháp, thôn tính các tỉnh Alsace và Loraine và chấm dứt sự thống trị của Pháp ở châu Âu. Sau đó, sự đe dọa triền miên của nước Đức liên bang dường như đã thúc đẩy các nhà giải mã Pháp phải làm chủ những kỹ năng cần thiết để cung cấp cho nước Pháp những thông tin tình báo chi tiết về các kế hoạch của kẻ thù.

Cũng trong khoảng thời gian đó, Auguste Kerckhoffs đã viết chuyên luận *La Cryptographie militaire* (Mật mã quân sự). Mặc dù Kerckhoffs là người Đức song ông sống hầu hết cuộc đời mình ở Pháp, và chuyên luận của ông đã cung cấp cho người Pháp một chỉ dẫn tuyệt vời về các nguyên tắc giải mã. Ba thập kỷ sau, vào lúc Thế chiến Thứ nhất bắt đầu, quân đội Pháp đã thực hiện các ý tưởng của Kerckhoffs ở quy mô công nghiệp. Trong khi các thiên tài đơn thương độc mã như Painvin cặm cụi để hóa giải các loại mật mã mới thì các nhóm chuyên gia, mỗi nhóm chuyên phát triển những kỹ năng để giải quyết một loại mật mã cụ thể, tập trung vào việc giải mã hằng ngày. Thời gian là cực kỳ quan trọng, và việc giải mã theo kiểu dây chuyền có thể cung cấp thông tin tình báo một cách nhanh chóng và hiệu quả.

Trung úy Georges Painvin

Tôn Tử, tác giả của cuốn *Binh pháp*, một cuốn sách viết về chiến lược quân sự ở thế kỷ thứ 4 trước Công nguyên, đã nói: "Trong ba quân, xét chung những người thân thiết với tướng súy thì không ai thân thiết cho bằng gián điệp, xét chung những kẻ được thưởng

thì không ai được thưởng nhiều cho bằng gián điệp, xét chung các việc bí mật thì không việc nào bí mật cho bằng gián điệp". Người Pháp là những người tin tưởng nồng nhiệt vào những lời dạy của Tôn Tử, và ngoài việc mài giũa các kỹ năng giải mã của mình, họ còn phát minh ra một số kỹ thuật trợ giúp cho việc thu thập thông tin tình báo vô tuyến, những phương pháp không có liên quan gì đến việc giải mã. Chẳng hạn, người Pháp nghe tin để học cách nhận ra *tay máy (fist)* của các điện báo viên. Một khi đã được mã hóa, bức thư được gửi đi bằng mã Morse, gồm một chuỗi các dấu chấm và gạch, và mỗi điện báo viên đều có thể được nhận biết nhờ những khoảng ngắt, tốc độ truyền, và độ dài tương đối của dấu chấm và dấu gạch. Tay máy cũng tương tự như chữ viết tay đều có thể nhận biết được. Cùng với việc nghe tin, người Pháp còn thiết lập sáu trạm dò hướng để tìm ra thông tin được truyền đến từ đâu. Mỗi trạm xoay ăngten cho đến khi tín hiệu nhận được là mạnh nhất, từ đó xác định được một hướng của nguồn thông tin. Bằng cách tổng hợp các thông tin về hướng của hai hoặc một số trạm người ta sẽ định vị được vị trí truyền tin chính xác của đối phương. Việc kết hợp giữa thông tin về tay máy và thông tin về hướng, có thể xác định được cả nhận dạng con người lẫn vị trí của một tiểu đoàn. Tình báo của Pháp sau đó có thể lần ngược lại trong vòng vài ngày và có khả năng tìm ra đích cũng như mục tiêu của nó. Dạng thu thập thông tin tình báo này, được gọi là phân tích đường truyền tin, rất có giá trị, đặc biệt là khi xuất hiện một loại mật mã mới. Mỗi dạng mật mã mới có thể nhất thời khiến các nhà giải mã bất lực, song ngay cả khi một bức thư không giải mã được cũng có thể mang lại thông tin nào đó qua việc phân tích đường truyền.

Sự thận trọng của người Pháp tương phản rõ nét với thái độ của người Đức, họ tham gia vào chiến tranh mà không có văn phòng giải mã của quân đội. Mãi cho đến năm 1916, họ mới thành lập Abhorchdienst, một cơ quan phục vụ cho việc chặn bắt thư từ của quân Đồng minh. Một phần lý do của việc chậm thành lập Abhorchdienst đó là quân đội Đức ngay từ đầu cuộc chiến đã tiến trước vào lãnh thổ của Pháp. Để đối phó lại, người Pháp đã phá hủy các phương tiện viễn thông trên bộ, buộc toán quân Đức đi trước phải liên lạc qua vô tuyến. Trong khi điều này giúp cho người Pháp liên tục chặn bắt được thông tin của quân Đức, thì phía đối phương lại không làm được như vậy. Khi Pháp lui quân vào sâu lãnh thổ của mình, họ vẫn có thể sử dụng phương tiện viễn thông của họ và không phải liên lạc qua vô tuyến. Vì quân Pháp không sử dụng vô tuyến trong liên lạc nên quân Đức không bắt được thông tin nào và vì vậy họ đã không chú ý đến việc thiết lập một bộ phận giải mã cho mãi đến hai năm sau trong cuộc chiến.

Người Anh và người Mỹ cũng có những đóng góp quan trọng cho công việc giải mã của quân Đồng minh. Tầm quan trọng bậc nhất của các nhà giải mã của quân Đồng minh và ảnh hưởng của họ đến cuộc chiến tranh được minh họa rõ nhất trong việc giải mã một bức điện tín của quân Đức bị quân Anh bắt được ngày 17 tháng Một năm 1917. Sự việc này đã cho thấy khoa giải mã có thể ảnh hưởng ở mức độ cao nhất đến tiến trình của cuộc chiến tranh như thế nào, và minh họa cho hậu quả khủng khiếp có thể xảy ra nếu sử dụng loại mật mã không thích hợp. Trong vòng vài tuần, bức điện tín được giải mã đã khiến người Mỹ phải suy nghĩ lại chính sách trung lập của mình, nhờ đó đã mang lại thế cân bằng cho cuộc chiến.

Mặc cho sự kêu gọi từ các chính trị gia Anh và Mỹ, trong hai năm đầu của cuộc chiến tranh, Tổng thống Woodrow Wilson vẫn kiên quyết từ chối không gửi binh lính Mỹ tăng cường cho quân Đồng minh. Ngoài chuyện không muốn hy sinh thế hệ trẻ của quốc gia vào chiến trường đẫm máu ở châu Âu, ông ta còn cho rằng cuộc chiến tranh chỉ có thể kết thúc thông qua đàm phán và tin rằng ông ta có thể cống hiến tốt nhất cho thế giới khi vẫn đứng trung lập như một người trung gian hòa giải. Tháng Mười một năm 1916, Wilson đã nhận thấy có hy vọng về một cuộc thu xếp bằng đàm phán khi Đức bổ nhiệm Ngoại trưởng mới, Arthur Zimmermann, một người đàn ông cao lớn vui tính, dường như báo hiệu một thời đại mới của chính sách ngoại giao tiến bộ ở Đức. Báo chí Mỹ chạy những hàng tít lớn như *Zimmermann người bạn của chúng ta và Sự Tự do hóa nước Đức*, và một bài báo đã coi ông ta là "một trong những điềm lành thuận lợi nhất cho tương lai của quan hệ Đức - Mỹ". Tuy nhiên, người Mỹ không biết rằng, Zimmermann không hề có ý định theo đuổi hòa bình. Thay vào đó, ông ta âm mưu mở rộng sự xâm lược của quân đội Đức.

Trở lại năm 1915, một chiếc tàu ngầm Đức đã làm đắm tàu chở khách *Lusitania*, khiến cho 1.198 hành khách, trong đó có 128 công dân Mỹ bị thiệt mạng. Vụ việc này lẽ ra đã khiến Mỹ phải nhảy vào cuộc chiến nếu như không có lời cam kết từ phía Đức rằng sau này tàu ngầm của Đức sẽ nổi lên trên mặt biển trước khi tấn công, một sự hạn chế nhằm tránh tấn công nhầm vào các tàu dân sự. Tuy nhiên, ngày 9 tháng Một năm 1917, Zimmermann đã tham dự một cuộc họp quan trọng tại Lâu đài Pless ở Đức, tại đây Bộ Chỉ huy Tối cao đã cố gắng thuyết phục Kaiser rằng đã đến lúc từ bỏ lời cam kết và bắt đầu một thời kỳ chiến tranh tàu ngầm

không hạn chế. Các sĩ quan chỉ huy của Đức biết rằng tàu ngầm của họ hầu như không thể bị tổn hại nếu họ phóng ngư lôi khi còn đang chìm dưới nước, và họ tin rằng điều này sẽ chứng minh đó là yếu tố tích cực quyết định đến kết cục của cuộc chiến. Đức đã thành lập một hạm đội gồm hai trăm tàu ngầm và Bộ Chỉ huy Tối cao cho rằng cuộc xâm lược bằng tàu ngầm không hạn chế sẽ cắt đứt các đường tiếp viện cho Anh và buộc họ phải khuất phục trong vòng 6 tháng.

Arthur Zimmermann

Một chiến thắng chớp nhoáng là cực kỳ quan trọng. Cuộc chiến tàu ngầm không hạn chế và những vụ làm đắm tàu dân sự Mỹ không thể tránh khỏi gần như chắc chắn sẽ khiến Mỹ tuyên bố chiến tranh với Đức. Chính vì vậy, Đức cần phải buộc quân Đồng minh đầu hàng trước khi Mỹ có thể tập hợp quân và gây ảnh hưởng lớn đến vũ đài châu Âu. Kết thúc cuộc họp tại Pless, Kaiser đã bị thuyết phục rằng một chiến thắng chớp nhoáng là có thể đạt được, và ông ta đã ký lệnh cho phép mở cuộc chiến tàu ngầm không hạn chế, có hiệu lực từ ngày 1 tháng Hai.

Trong ba tuần còn lại, Zimmermann đã lập ra một chính sách bảo hiểm. Nếu cuộc chiến tàu ngầm không hạn chế khiến Mỹ chắc chắn sẽ tham gia vào chiến tranh, thì Zimmermann đã có

một kế hoạch gây trì hoãn và làm yếu đi sự can thiệp của Mỹ vào châu Âu, và thậm chí có thể còn ngăn cản hoàn toàn ý định đó. Ý tưởng của Zimmermann là đề xuất liên minh với Mexico, và thuyết phục Tổng thống Mexico tấn công Mỹ và chiếm lại các vùng như Texas, New Mexico và Arizona. Đức cũng sẽ hỗ trợ Mexico trong cuộc chiến với kẻ thù chung, cả về tài chính lẫn quân sự.

Thêm nữa, Zimmermann muốn tổng thống Mexico làm trung gian thuyết phục Nhật Bản cùng tấn công nước Mỹ. Bằng cách này, Đức sẽ đặt mối đe dọa đối với bờ phía đông của nước Mỹ, Nhật tấn công từ phía tây và Mexico xâm lược ở phía nam. Động cơ chính của Zimmermann là buộc Mỹ phải đối phó với những khó khăn của chính mình để không còn đủ khả năng đem quân tới châu Âu nữa. Nhờ đó Đức có thể giành chiến thắng trong cuộc chiến trên biển và cuộc chiến ở châu Âu, rồi sau đó sẽ rút ra khỏi chiến dịch ở Mỹ. Ngày 16 tháng Một, Zimmermann đã tóm tắt kế hoạch của mình trong một bức điện gửi cho Đại sứ Đức tại Washington, người này có nhiệm vụ chuyển kế hoạch đó cho Đại sứ Đức ở Mexico để gửi Tổng thống Mexico. Hình 28 trình bày bức điện tín đã được mã hóa; nội dung của bức điện đó như sau:

> Chúng ta dự định bắt đầu cuộc chiến tàu ngầm không hạn chế vào đầu tháng Hai. Mặc dù vậy, bằng mọi cách chúng ta phải cố gắng giữ vị trí trung lập của Mỹ. Trong trường hợp không thành công, chúng ta sẽ đề nghị Mexico hợp tác trên nguyên tắc cơ bản: cùng thực hiện chiến tranh, cùng thực hiện hòa bình, hỗ trợ tài chính rộng rãi, và một sự cảm thông của phía chúng ta đối với mong muốn được tái chiếm những vùng lãnh thổ đã

mất của Mexico như Texas, New Mexico và Arizona. Việc thu xếp chi tiết sẽ do ông quyết định.

Ông hãy thông báo cho Tổng thống (của Mexico) về những điều trên đây một cách tối mật, ngay khi chiến tranh với Mỹ là chắc chắn nổ ra, và bổ sung thêm khuyến nghị rằng, ông ta hãy mời Nhật Bản, theo sáng kiến của ông ta, liên minh ngay lập tức và đồng thời làm trung gian giữa Nhật Bản và chúng ta.

Ông hãy lưu ý Tổng thống rằng thực tế việc chúng ta bắt đầu cuộc chiến tranh tàu ngầm không hạn chế lúc này sẽ mang lại triển vọng buộc Anh phải tiến tới hòa bình trong vòng vài tháng. Hãy báo cho tôi biết ông đã nhận được bức điện này.

Zimmermann

Zimmermann đã mã hóa bức điện của mình vì Đức biết quân Đồng minh chặn bắt được tất cả các thông tin qua Đại Tây dương, một hệ quả của hành động tấn công đầu tiên của Anh trong cuộc chiến. Trước bình minh ngày đầu tiên của Thế chiến Thứ nhất, tàu *Telconia* của Anh đã xâm nhập vào bờ biển nước Đức nhờ có bóng tối che phủ, nó thả neo và kéo lên các dây cáp ở dưới biển. Đó là các dây cáp của Đức đi xuyên qua Đại Tây dương - mối liên kết thông tin giữa Đức với phần còn lại của thế giới. Vào lúc mặt trời mọc thì tất cả các đường cáp đều đã bị cắt đứt. Hành động phá hoại ngầm này là nhằm phá hủy phương tiện liên lạc an toàn nhất của Đức, buộc Đức phải gửi thư từ qua các đường liên lạc bằng sóng vô tuyến không mấy an toàn hoặc qua các đường cáp của nước khác. Zimmermann buộc phải gửi bức điện của mình qua đường cáp của Thụy điển và để phòng xa, ông ta còn gửi trực tiếp qua đường cáp của Mỹ. Cả hai con đường đều qua Anh, và

cũng có nghĩa là bức điện tín Zimmermann, như ngày nay vẫn gọi, nhanh chóng rơi vào tay quân Anh.

Bức điện ngay lập tức được chuyển đến Phòng 40, phòng mật mã Bộ Hải quân Anh. Phòng 40 là một hỗn hợp người kỳ lạ, nó gồm các nhà ngôn ngữ, các học giả cổ văn và những người mê giải câu đố, có khả năng lập những chiến công tài tình nhất trong việc giải mã. Chẳng hạn, Reverend Montgomery, một dịch giả tài năng các tác phẩm thần học của Đức, đã giải mã được bức thư bí mật giấu trong một tấm bưu thiếp gửi Ngài Henry Jones, 184 đường King's Road, Tighnabruaich, Scotland. Tấm bưu thiếp được gửi từ Thổ Nhĩ Kỳ, nên Ngài Henry đoán rằng nó là của người con trai ông, bị giam ở nhà tù Thổ Nhĩ Kỳ gửi về. Tuy nhiên, ông thấy bối rối vì tấm bưu thiếp để trắng và địa chỉ cũng kỳ lạ - làng Tighnabruaich quá nhỏ nên không có nhà nào được đánh số và cũng không có đường King's Road nào hết. Cuối cùng thì Reverend Montgomery nhận ra đó chính là bức thư mã hóa trên tấm bưu thiếp. Dòng địa chỉ ở đây là muốn nói tới một đoạn trong cuốn Kinh thánh, Sách thứ nhất về các Vua, Chương 18, Câu 4: "Obadiah có đem một trăm đấng tiên tri đi giấu trong hai hang đá, mỗi hang năm mươi người, dùng bánh mì và nước mà nuôi họ". Con trai của Ngài Henry chỉ đơn giản là muốn gia đình yên tâm rằng anh ta vẫn được những kẻ giam giữ chăm sóc tốt.

Khi bức điện Zimmermann đến Phòng 40, chính Montgomery là người chịu trách nhiệm giải mã nó cùng với Nigel de Grey, một chủ nhà xuất bản được hãng William Heinemann phái tới. Họ ngay lập tức nhận ra rằng mình đang phải đương đầu với một dạng mật mã chỉ được sử dụng trong những liên lạc ngoại giao cao cấp, và họ rất khẩn trương bắt tay giải mã. Việc giải mã

hoàn toàn không dễ dàng song họ lợi dụng được những kết quả phân tích các bức điện được mã hóa trước đây. Trong vòng vài giờ, hai nhà giải mã đã phục hồi được một số đoạn trong văn bản, đủ để hiểu rằng họ đang giải mã một bức thư cực kỳ quan trọng. Montgomery và de Grey đã kiên trì thực hiện nhiệm vụ của mình và hết ngày hôm đó, họ đã hiểu được sơ lược những kế hoạch khủng khiếp của Zimmermann. Họ nhận thấy những hậu quả đầy chết chóc của cái gọi là chiến tranh tàu ngầm không hạn chế, nhưng đồng thời họ cũng hiểu rằng vị ngoại trưởng Đức này đang khuyến khích một kế hoạch tấn công nước Mỹ, mà điều này có nhiều khả năng sẽ khiến Tổng thống Wilson từ bỏ vai trò trung lập của mình. Bức điện còn chứa đựng các mối đe dọa khủng khiếp nhất song cũng tính đến khả năng Mỹ gia nhập Đồng minh.

Montgomery và de Grey đã gửi một phần bức điện được giải mã cho Đô đốc, Ngài William Hall, Giám đốc Cục tình báo hải quân, với mong muốn ông sẽ chuyển thông tin này cho phía Mỹ, nhờ đó có thể lôi kéo họ tham gia cuộc chiến. Tuy nhiên, Đô đốc Hall chỉ đơn giản cất nó vào két sắt và yêu cầu các nhà giải mã tiếp tục hoàn thiện nốt những phần còn bỏ trống. Ông do dự không muốn chuyển cho phía Mỹ bức điện chưa được giải mã hoàn chỉnh, vì e rằng còn có những thông tin quan trọng vẫn chưa được giải mã. Thực ra, ông cũng có một mối lo ngại khác lẩn quất trong đầu. Nếu nước Anh đưa bức điện Zimmermann đã được giải mã cho phía Mỹ thì những người Mỹ sẽ phản ứng lại bằng cách công khai chỉ trích kế hoạch xâm lược của Đức, và người Đức sẽ rút ra ngay kết luận rằng phương pháp mã hóa của họ đã bị hóa giải. Điều này sẽ khiến họ phải phát triển một

hệ thống mật mã mới mạnh hơn, do đó sẽ làm mất đi một kênh tình báo quan trọng. Vả lại, Hall cũng hiểu rằng cuộc tấn công tổng lực bằng tàu ngầm sẽ diễn ra chỉ trong vòng hai tuần nữa, mà chỉ nội điều đó thôi cũng đủ để khiến Tổng thống Wilson tuyên bố chiến tranh với Đức. Do đó không việc gì mà phải làm phương hại đến một nguồn tin tình báo giá trị, khi mà kết cục mong muốn dù thế nào cũng sẽ xảy ra.

Hình 28. Bức điện của Zimmermann, được von Bernstorff, Đại sứ Đức tại Washington gửi cho Eckhardt, Đại sứ Đức tại Mexico City.

Ngày 1 tháng Hai, theo lệnh của Kaiser, quân Đức khởi động cuộc chiến tranh hải quân không hạn chế. Ngày 2 tháng Hai, Woodrow Wilson chủ trì một cuộc họp nội các để quyết định phản ứng của Mỹ. Ngày 3 tháng Hai, ông ta tuyên bố với Quốc hội và thông báo rằng Mỹ sẽ vẫn tiếp tục giữ vị trí trung lập với tư cách là người thiết lập hòa bình, không tham chiến. Điều này đi ngược lại với mong đợi của quân Đồng minh và Đức. Việc Mỹ do dự gia nhập Đồng minh đã buộc Đô đốc Hall không còn lựa chọn nào khác là phải dùng đến bức điện Zimmermann.

Trong vòng hai tuần kể từ khi Montgomery và de Grey lần đầu tiên báo cáo với Hall, họ đã hoàn thành việc giải mã. Thêm vào đó, Hall đã tìm ra cách khiến quân Đức không nghi ngờ gì về việc bí mật của họ đã bị phát lộ. Ông biết rằng von Bernstorff, Đại sứ Đức tại Washington, sẽ chuyển bức điện cho von Eckhardt, Đại sứ Đức tại Mexico, sau khi đã có một vài thay đổi nhỏ. Chẳng hạn, von Bernstorff sẽ bỏ đi những chỉ thị riêng cho ông ta và thay đổi địa chỉ. Von Eckhardt sau đó sẽ chuyển bức điện đã sửa đổi và đã được giải mã này cho Tổng thống Mexico. Nếu Hall bằng cách nào đó có được bức điện gửi đến Mexico thì nó có thể được công bố và người Đức sẽ cho rằng nó đã bị đánh cắp từ chỗ Chính phủ Mexico, chứ không phải bị người Anh chặn bắt được trên đường gửi tới Mỹ và giải mã nó. Hall liên lạc với điệp viên của mình ở Mexico, với biệt danh là Mr. H, và người này sẽ có nhiệm vụ đột nhập Cục Điện báo Mexico, để lấy chính xác thứ mà Hall cần - đó là bức điện Zimmermann gửi chính phủ Mexico.

Đây cũng chính là bức điện mà Hall đã chuyển tới Arthur Balfour, Ngoại trưởng Anh. Ngày 23 tháng Hai, Balfour đã mời Đại sứ Mỹ, Walter Page tới và đưa cho ông ta xem bức điện

Zimmermann, mà sau này ông đã gọi đó là "giây phút quan trọng nhất trong cuộc đời tôi". Bốn ngày sau, Tổng thống Wilson đã tận mắt nhìn thấy cái mà ông gọi là "bằng chứng hùng hồn", chứng tỏ Đức đang rắp tâm mở rộng xâm lược trực tiếp vào Mỹ.

Bức điện cũng đã được công bố cho giới báo chí, và cuối cùng thì Mỹ cũng phải đối diện với thực tế trước những mưu đồ của Đức. Mặc dù vậy, những người dân Mỹ vẫn nghi ngại việc cần phải trả đũa và bên trong chính quyền Mỹ vẫn còn lo ngại rằng bức điện này có thể là một trò lừa đảo, được người Anh bày ra để buộc Mỹ phải tham chiến. Tuy nhiên, sự nghi ngờ về tính xác thực mau chóng biến mất khi Zimmermann công khai thừa nhận trách nhiệm của mình. Tại một cuộc họp báo ở Berlin, không hề bị sức ép nào, ông ta chỉ đơn giản tuyên bố: "Tôi không thể chối bỏ điều này. Đó là sự thật".

Hình 29 "Nổ tung trong tay ông ta", tranh biếm họa của Rollin Kirby in trên tạp chí *Thế giới* ngày 3 tháng Ba năm 1917.

Ở Đức, Bộ ngoại giao đã tiến hành một cuộc điều tra xem bằng cách nào Mỹ đã có được bức điện Zimmermann. Họ đã bị rơi vào bẫy của Hall và đi đến kết luận rằng "những bằng chứng khác nhau đều cho thấy sự rò rỉ là từ phía Mexico". Trong khi đó, Hall vẫn tiếp tục làm giảm bớt sự chú ý tới công việc của các nhà giải mã Anh. Ông dựng nên một câu chuyện cho giới báo chí Anh nhằm chỉ trích tổ chức của chính ông đã không chặn bắt được bức điện của Zimmermann, dẫn tới việc hàng loạt bài báo tấn công vào lực lượng tình báo của Anh và tán dương Mỹ.

Vào đầu năm, Wilson đã từng nói rằng sẽ là một "tội ác đối với dân tộc" nếu để đất nước của ông ta tham chiến, nhưng đến ngày 2 tháng Tư năm 1917, ông ta đã thay đổi quyết định: "Tôi xin khuyến nghị Quốc hội nên tuyên bố rằng đường lối mới đây của Chính phủ Đế quốc (tức Chính phủ Đức - ND) thực tế không gì khác là đang thực hiện cuộc chiến tranh chống lại chính phủ và nhân dân Hoa Kỳ, và nên chính thức chấp nhận tình trạng tham chiến để đẩy lùi cuộc chiến tranh đó". Một thành công duy nhất mà các nhà giải mã Phòng 40 đã đạt được chính ở chỗ mà ba năm ngoại giao tích cực đều thất bại. Barbara Tuchman, nhà sử học Mỹ và là tác giả cuốn *Bức điện Zimmermann*, đã phân tích như sau:

> Nếu bức điện này không bị chặn bắt hoặc không được công bố thì người Đức tất đã làm được điều gì đó trước khi buộc chúng ta cuối cùng phải tham chiến. Nhưng nếu như vậy thì đã quá muộn. Nếu chúng ta trì hoãn lâu hơn nữa thì quân Đồng minh có thể đã bị buộc phải thương lượng. Trên phương diện đó, thì bức điện Zimmermann đã làm thay đổi cả tiến trình lịch sử... Bản thân bức điện Zimmermann cũng chỉ là một viên sỏi trên

con đường dài của lịch sử. Nhưng một viên sỏi có thể giết chết gã khổng lồ Goliath, và chính viên sỏi này đã giết chết những ảo tưởng của người Mỹ khi nghĩ rằng chúng ta có thể vui vẻ đi con đường của riêng mình tách biệt với các quốc gia khác. Trong các sự kiện của thế giới thì đây chỉ là một âm mưu nhỏ của một Ngoại trưởng Đức. Còn trong cuộc sống của người dân Mỹ thì đó là kết thúc của sự ngây thơ.

Báu vật của Khoa học mật mã

Cuộc Chiến tranh Thế giới Thứ nhất đã chứng kiến một loạt chiến thắng của các nhà giải mã, kết thúc là việc giải mã bức điện Zimmermann. Kể từ khi hóa giải được mật mã Vigenère vào thế kỷ 19, các nhà giải mã vẫn ở trên thế thượng phong so với các nhà tạo mã. Vì vậy, cho đến khi kết thúc chiến tranh, khi các nhà tạo mã đang trong tình trạng cực kỳ tuyệt vọng, thì các nhà khoa học Mỹ đã có một đột phá đáng kinh ngạc. Họ khám phá ra rằng mật mã Vigenère có thể được sử dụng làm cơ sở cho một dạng mật mã mới, khó vượt qua hơn. Thực tế, mật mã mới này có thể đem lại độ an toàn tuyệt đối.

Điểm yếu căn bản của mật mã Vigenère là bản chất quay vòng của nó. Nếu từ khóa có năm chữ cái thì mỗi chữ cái thứ năm trong văn bản thường lại được mã hóa theo cùng một bảng chữ cái mật mã. Nếu người giải mã có thể xác định được số chữ cái trong từ khóa mã thì văn bản mật mã có thể được xử lý như là một tập hợp của năm mật mã dùng một bảng chữ cái, và mỗi mật mã có thể được hóa giải bằng phương pháp phân tích tần suất. Tuy nhiên, hãy thử xem điều gì sẽ xảy ra nếu từ khóa mã có nhiều chữ cái hơn.

Hãy tưởng tượng một văn bản thường gồm 1.000 chữ cái được mã hóa theo mật mã Vigenère, và chúng ta đang thử giải bản mật mã đó. Nếu từ khóa mã được sử dụng để mã hóa chỉ có năm chữ cái, thì bước cuối cùng của việc giải mã là áp dụng phương pháp phân tích tần suất đối với năm nhóm, mỗi nhóm chứa 200 chữ cái và việc này thật dễ dàng. Nhưng nếu từ khóa mã gồm 20 chữ cái, thì bước cuối cùng là áp dụng phương pháp phân tích tần suất đối với 20 nhóm, mỗi nhóm chứa 50 chữ cái, việc này đã khó hơn một cách đáng kể. Và nếu từ khóa mã có 1000 chữ cái thì bạn phải phân tích tần suất của 1000 nhóm, mỗi nhóm chứa 1 chữ cái, và điều này thì hoàn toàn không thể thực hiện được. Nói cách khác, nếu từ khóa mã (hay cụm từ khóa mã) có số chữ cái bằng với văn bản thường thì kỹ thuật giải mã của Babbage và Kasiski sẽ trở nên vô dụng.

Sử dụng một từ khóa mã có độ dài bằng với văn bản thì càng tốt nhưng điều này đòi hỏi người mã hóa phải tạo được một từ khóa mã thật dài. Nếu văn bản gồm hàng trăm chữ cái thì khóa mã cũng cần có đến hàng trăm chữ cái. Thay vì chọn ngẫu nhiên để tạo ra khóa mã, ta có thể thử lấy, chẳng hạn, lời một bài hát. Hoặc người mã hóa lấy từ một cuốn sách viết về nhận dạng chim và tạo khóa mã bằng cách chọn tên các loại chim một cách ngẫu nhiên. Tuy nhiên, những khóa mã như vậy vẫn còn những sơ hở rất cơ bản.

Trong ví dụ dưới đây, tôi mã hóa một câu bằng mật mã Vigenère với cụm từ khóa mã được sử dụng có độ dài bằng với câu gốc. Tất cả các kỹ thuật giải mã mà tôi trình bày ở trên đều thất bại. Tuy nhiên, câu này vẫn có thể giải mã được.

Cụm từ khóa mã
? ?
Văn bản thường
? ?
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

Hệ thống giải mã mới bắt đầu bằng việc giả định rằng văn bản mật mã có chứa các từ thường gặp, như **the**, chẳng hạn. Sau đó, chúng ta đặt một cách ngẫu nhiên từ **the** ở những vị trí khác nhau trong văn bản thường, như trình bày dưới đây và tìm ra các chữ cái trong từ khóa mã cần để chuyển **the** thành các chữ cái tương ứng trong văn bản mật mã. Chẳng hạn, nếu chúng ta giả định rằng **the** là từ đầu tiên trong văn bản thường, thì có thể suy ra điều gì về ba chữ cái đầu tiên của từ khóa mã? Chữ cái đầu tiên trong từ khóa mã sẽ mã hóa **t** thành **V**. Để tìm ra chữ cái đầu tiên trong từ khóa mã, chúng ta sử dụng hình vuông Vigenère, nhìn vào cột bắt đầu bằng chữ **t** cho đến khi thấy **V**, rồi tìm chữ chữ cái bắt đầu của dòng chứa chữ **V** đó, ta sẽ tìm được chữ cái đó là **C**. Lặp lại quá trình này với **h** và **e** được mã hóa thành **H** và **R** tương ứng, và cuối cùng chúng ta tìm được ba chữ cái đầu tiên của từ khóa mã là **CAN**. Tất cả có được là nhờ ta đã giả định **the** là từ đầu tiên trong văn bản thường. Đặt **the** vào một số vị trí khác và một lần nữa, lại tìm được các chữ cái tương ứng trong từ khóa mã (Bạn có thể kiểm tra mối quan hệ giữa mỗi chữ cái trong văn bản thường và văn bản mật mã bằng cách tham khảo hình vuông Vigenère ở Bảng 9).

Khóa mã
C A N ? ? ? B S J ? ? ? ? ? Y P T ? ? ? ?
Văn bản thường
t h e ? ? ? t h e ? ? ? ? ? t h e ? ? ? ?
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

Chúng ta thử đặt ba từ **the** vào ba chỗ ngẫu nhiên của văn bản mật mã, và có được ba nhóm chữ cái giả định ở những phần nhất định của từ khóa mã. Vậy làm thế nào biết được từ **the** nào ở vị trí đúng? Chúng ta đoán rằng từ khóa mã chứa các từ có nghĩa và đó là điểm lợi thế cho chúng ta. Nếu một từ **the** ở vị trí sai thì có thể sẽ cho kết quả là tập hợp ngẫu nhiên các chữ cái trong từ khóa mã. Tuy nhiên, nếu nó ở vị trí đúng thì các chữ cái trong từ khóa mã sẽ tạo nên một nghĩa nào đó. Chẳng hạn, chữ **the** đầu tiên cho các chữ cái trong từ khóa mã là **CAN,** điều này thật đáng khích lệ, vì đây là một âm tiết tiếng Anh hoàn toàn hợp lý. Như vậy, có thể từ **the** này ở vị trí đúng. Từ **the** thứ hai cho nhóm chữ cái **BSJ**, là một tập hợp quá đặc biệt của các phụ âm, cho thấy từ **the** thứ hai này có thể không đúng. Từ **the** thứ ba cho các chữ cái **YPT**, một âm tiết không bình thường nhưng cũng đáng để nghiên cứu tiếp. Nếu **YPT** thực sự là một phần cấu tạo nên từ khóa mã thì nó có thể thuộc một từ dài hơn, mà chỉ có thể là các khả năng **APOCALYPTIC, CRYPT** và **EGYPT**, và các từ phái sinh của các từ này. Làm thế nào chúng ta xác định được từ nào trong số các từ trên là thuộc từ khóa mã? Chúng ta có thể kiểm tra thử mỗi khả năng bằng cách chèn ba ứng viên trên vào từ khóa mã, bên trên đoạn thích hợp của văn bản mật mã và tìm ra các chữ cái tương ứng trong văn bản thường:

Khóa mã
C A N ? ? ? ? ? A P O C A L Y P T I C ? ?
Văn bản thường
t h e ? ? ? ? ? n q c b e o t h e x g ? ?
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

Khóa mã
C A N ? ? ? ? ? ? ? ? ? C R Y P T ? ? ? ?
Văn bản thường
t h e ? ? ? ? ? ? ? ? ? c i t h e ? ? ? ?
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

Khóa mã
C A N ? ? ? ? ? ? ? ? ? E G Y P T ? ? ? ?
Văn bản thường
t h e ? ? ? ? ? ? ? ? ? a t t h e ? ? ? ?
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

Nếu từ được thử không thuộc từ khóa mã thì nó có thể sẽ cho kết quả là một nhóm các chữ cái vô nghĩa trong văn bản thường, nhưng nếu nó thuộc từ khóa mã thì các chữ cái trong văn bản thường phải tạo nên các từ có nghĩa. Với **APOCALYPTIC** thì kết quả là nhóm các chữ cái đó là cực kỳ vô nghĩa. Với **CRYPT**, kết quả là **cithe**, cũng không phải là một nhóm từ không thể chấp nhận được. Tuy nhiên, nếu **EGYPT** thuộc từ khóa mã thì nó cho nhóm chữ cái **atthe**, một sự kết hợp các chữ cái có vẻ hứa hẹn hơn, có thể đó là các từ **at the**.

Đến đây, chúng ta hãy giả sử rằng khả năng chắc chắn nhất là **EGYPT** thuộc từ khóa mã. Có lẽ khóa mã ở đây là một danh sách tên các nước. Điều này gợi ý rằng **CAN**, nhóm chữ cái thuộc

khóa mã tương ứng với chữ **the** đầu tiên, có thể là các chữ cái bắt đầu của từ **CANADA**. Chúng ta có thể thử giả định này bằng cách tìm thêm các chữ cái của văn bản thường dựa trên từ giả định **CANADA** và **EGYPT** thuộc khóa mã:

Khóa mã
C A N A D A ? ? ? ? ? ? E G Y P T ? ? ? ?
Văn bản thường
t h e m e e ? ? ? ? ? ? a t t h e ? ? ? ?
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

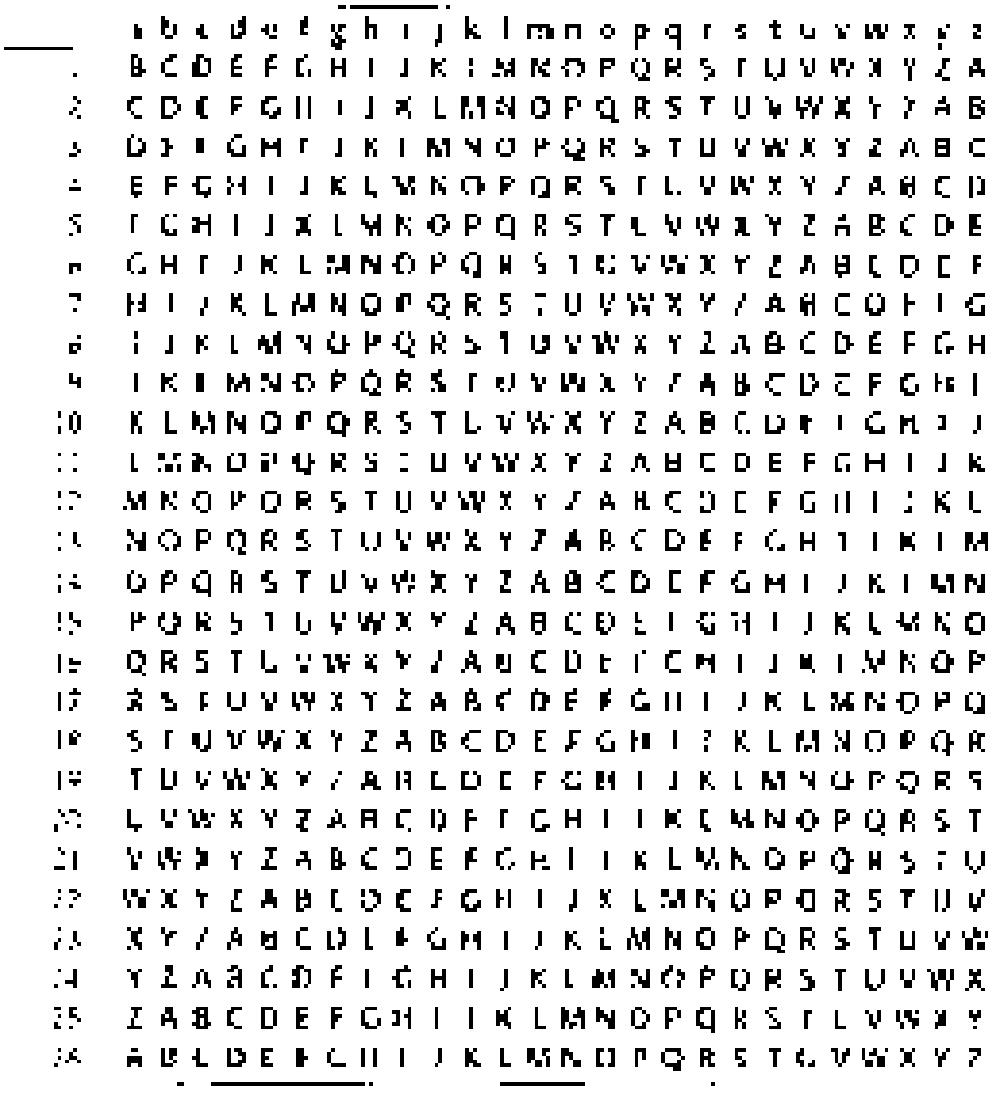
Giả định của chúng ta có vẻ hợp lý. **CANADA** cho ta các chữ cái bắt đầu của văn bản thường là **themee**, có lẽ là **the meeting**. Giờ thì chúng ta tìm ra thêm được một số chữ cái nữa của văn bản thường, đó là **ting**, từ đó suy ra các chữ cái tương ứng trong khóa mã, đó là **BRAZ**. Chắc chắn đây là các chữ cái bắt đầu của từ **BRAZIL**. Sử dụng tập hợp các từ **CANADABRAZILEGYPT**, chúng ta có được phần giải mã sau: **the meeting is at the????**.

Để tìm từ cuối cùng trong văn bản thường, địa điểm của cuộc gặp (the meeting), phương cách tốt nhất là hoàn tất từ khóa mã bằng cách thử tên của tất cả các quốc gia có thể và suy ra các chữ cái còn lại của văn bản thường. Chỉ có một khả năng hợp lý khi nhóm chữ cái cuối cùng của từ khóa mã là **CUBA:**

Khóa mã
C A N A D A B R A Z I L E G Y P T C U B A
Văn bản thường
t h e m e e t i n g i s a t t h e d o c k
Văn bản mật mã
V H R M H E U Z N F Q D E Z R W X F I D K

Như vậy, một khóa mã có số chữ cái bằng với văn bản chưa chắc đã đảm bảo đủ an toàn. Sự không an toàn trong ví dụ nêu trên nảy sinh vì (cụm) từ khóa mã được cấu tạo bởi các từ có nghĩa. Chúng ta bắt đầu bằng việc chèn ngẫu nhiên các từ **the** vào văn bản thường rồi tìm các chữ cái tương ứng trong từ khóa mã. Chúng ta có thể nói khi nào từ **the** được đặt vào vị trí đúng vì các chữ cái trong từ khóa mã dường như là một phần của những từ có nghĩa. Sau đó, chúng ta sử dụng những đoạn chữ cái đó để tìm ra toàn bộ các từ trong khóa mã. Đến lượt các từ này lại giúp chúng ta tìm ra thêm các đoạn chữ cái khác trong văn bản thường, nhờ đó chúng ta có thể mở rộng thêm ra các từ khác và cứ tiếp tục như vậy. Toàn bộ quá trình tới lui giữa văn bản thường và khóa mã này chỉ có thể thực hiện được khi từ khóa mã có một cấu trúc rõ ràng và gồm những từ có thể nhận ra. Tuy nhiên, năm 1918, các nhà mật mã đã bắt đầu thử nghiệm với các khóa mã không có cấu trúc nào cả. Và kết quả là thu được một mật mã không thể phá nổi.

Khi Thế chiến Thứ nhất đã gần đến hồi kết, Thiếu tá Joseph Mauborgne, giám đốc Viện Nghiên cứu Mật mã của quân đội Mỹ, đã đưa ra khái niệm về khóa mã ngẫu nhiên - nó không chứa một dãy các từ nào có thể nhận biết được mà chỉ là một dãy các chữ cái ngẫu nhiên. Ông đã ủng hộ việc áp dụng những khóa mã ngẫu nhiên này như một bộ phận của mật mã Vigenère để đạt được mức độ an toàn chưa từng có trước đó. Bước đầu tiên trong hệ thống của Mauborgne là soạn ra một quyển sổ tay dày, bao gồm hàng trăm trang, mỗi trang mang một khóa mã duy nhất dưới hình thức là hàng dãy các chữ cái được lựa chọn ngẫu nhiên. Quyển sổ tay này sẽ có hai bản, một cho người gửi và một

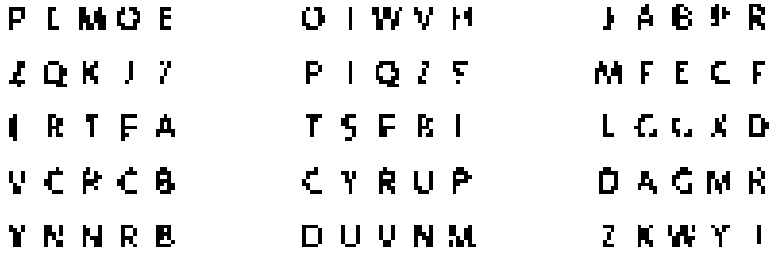


Bảng 9. Hình vuông Vigenère

cho người nhận. Để mã hóa một văn bản, người gửi sẽ sử dụng mật mã Vigenère với trang đầu tiên trong sổ tay làm khóa mã. Hình 30 trình bày ba trang từ một quyển sổ tay như vậy (trong thực tế mỗi trang chứa hàng trăm chữ cái), và phía dưới là một văn bản được mã hóa bằng cách sử dụng khóa mã ngẫu nhiên ở trang 1. Người nhận có thể dễ dàng giải mã bằng việc sử dụng đúng khóa mã đó và đảo ngược mật mã Vigenère. Một khi văn bản mật mã đó đã được gửi đi, nhận và giải mã xong, người gửi

và người nhận sẽ hủy trang đã sử dụng làm khóa mã, do vậy nó sẽ không bao giờ được sử dụng lại nữa. Khi văn bản tiếp theo được mã hóa, thì khóa mã ngẫu nhiên tiếp theo trong sổ tay được sử dụng và cuối cùng cũng bị hủy, và cứ tiếp tục như vậy. Vì mỗi khóa mã chỉ được sử dụng một lần và chỉ một lần duy nhất, nên hệ thống này còn được gọi là *mật mã sổ tay dùng một lần.*

Mật mã sổ tay dùng một lần khắc phục được tất cả các điểm yếu trước đây. Hãy thử tưởng tượng thông báo **attack the valley at dawn** *(tấn công thung lũng vào lúc bình minh)* được mã hóa như ở Hình 30, rồi gửi qua máy phát vô tuyến và bị kẻ thù chặn bắt được. Bản mật mã được chuyển tới cho các nhà giải mã. Chướng ngại đầu tiên đó là, theo định nghĩa, không có sự lặp lại nào trong khóa mã ngẫu nhiên, do vậy phương pháp của Babbage và Kasiski không thể nào phá được mật mã này. Một cách khác, các nhà giải



Khóa mã
P L M O E Z Q K J Z L R T E A V C R C B Y
Văn bản thường
a t t a c k t h e v a l i e y a t d a w n
Văn bản mật mã
P E F O G J J R N U L C E I Y V V U C X L

Hình 30. Ba trang, mỗi trang là một khóa mã tiềm năng đối với mật mã sổ tay dùng một lần. Văn bản ở đây được mã hóa với khóa mã ở trang 1.

mã đối phương có thể thử đặt từ **the** vào một số vị trí và tìm các chữ cái tương ứng của khóa mã, như chúng ta đã làm với đoạn văn bản trước. Nếu nhà giải mã đặt **the** vào đầu câu, mà như vậy là sai, thì những chữ cái tương ứng trong khóa mã sẽ là **WXB**, chỉ là dãy ngẫu nhiên các chữ cái mà thôi. Nếu nhà giải mã thử đặt **the** ở vị trí thứ bảy, vô tình là đúng, thì chữ cái trong khóa mã sẽ là **QKJ**, cũng chỉ là một đoạn chữ cái ngẫu nhiên. Nói cách khác, nhà giải mã không thể biết liệu các từ mình thử đặt vào có đúng vị trí hay không.

Trong cơn tuyệt vọng, nhà giải mã có thể nghĩ đến phương án thử tất cả các khóa mã có thể. Bản mật mã gồm 21 chữ cái, vì vậy nhà giải mã biết rằng khóa mã sẽ gồm 21 chữ cái. Điều này có nghĩa là cần phải thử 500.000.000.000.000.000.000.000.000.000 khóa mã khả dĩ, mà điều này hoàn toàn vượt quá khả năng của cả máy móc lẫn con người. Tuy nhiên, ngay cả khi nhà giải mã có thể thử hết tất cả các khả năng đi nữa, thì vẫn còn một khó khăn lớn hơn nữa phải vượt qua. Bằng cách kiểm tra tất cả các khóa mã khả dĩ, nhà giải mã chắc chắn sẽ tìm ra bức thư đúng - nhưng đồng thời cũng tìm ra tất cả các bức thư sai. Ví dụ, từ khóa mã dưới đây sử dụng để giải chính bản mật mã trên lại cho một bức thư hoàn toàn khác:

Khóa mã
M A A K T G Q K J N D R T I F D B H K T S
Văn bản thường
d e f e n d t h e h i l l a t s u n s e t
Văn bản mật mã
P E F O G J J R N U L C E I Y V V U C X L

(Bức thư được giải mã bây giờ lại là **defend the hill at sun set** - *phòng thủ ngọn đồi vào lúc mặt trời lặn).*

Nếu tất cả các khóa mã khác nhau đều được thử qua thì tất cả các bức thư gồm 21 chữ cái có nghĩa sẽ được tìm thấy và người giải mã sẽ không thể phân biệt được bức thư đúng với số còn lại. Khó khăn này sẽ không nảy sinh nếu từ khóa mã gồm một dãy các từ hoặc là một cụm từ, vì bức thư không đúng sẽ gần như chắc chắn gắn liền với khóa mã không có nghĩa, còn bức thư đúng sẽ ứng với khóa mã có nghĩa.

Độ an toàn của mật mã sổ tay dùng một lần là hoàn toàn dựa vào tính ngẫu nhiên của khóa mã. Khóa mã sẽ tạo nên tính ngẫu nhiên trong văn bản mật mã và nếu văn bản mật mã là ngẫu nhiên thì nó sẽ không hề có các hình mẫu, không có cấu trúc, tức không có gì để nhà giải mã bấu víu vào. Thực tế, có thể chứng minh bằng toán học rằng không có cửa nào cho người giải mã để giải một bức thư được mã hóa bằng mật mã sổ tay dùng một lần. Nói cách khác, mật mã sổ tay dùng một lần không chỉ được tin là không thể phá nổi, như mật mã Vigenère ở thế kỷ 19, *mà thực sự là nó tuyệt đối an toàn*. Mật mã sổ tay dùng một lần bảo đảm an toàn tuyệt đối: nó đúng là chiếc ly thánh của khoa mật mã.

Vậy là cuối cùng, các nhà tạo mã cũng đã tìm ra một hệ thống mật mã không thể phá nổi. Tuy nhiên, sự hoàn hảo của mật mã sổ tay dùng một lần vẫn không kết thúc được vấn đề giữ bí mật: sự thực của vấn đề là ở chỗ nó rất ít khi được sử dụng. Mặc dù về lý thuyết nó rất hoàn hảo, song lại có điểm yếu trong thực tế vì sử dụng mật mã này có hai khó khăn cơ bản. Thứ nhất, có một khó khăn thực tế trong việc soạn ra một số lượng lớn các khóa mã ngẫu nhiên. Trong một ngày, quân đội có thể phải trao đổi hàng trăm bức thư, mỗi bức thư lại bao gồm hàng ngàn ký tự, do vậy các điện báo viên sẽ phải được cung cấp các khóa mã hằng

ngày tương đương với hàng triệu các chữ cái được sắp xếp ngẫu nhiên. Cung cấp những chuỗi chữ cái ngẫu nhiên nhiều đến như vậy là một nhiệm vụ cực kỳ khó khăn.

Một số nhà mã hóa ban đầu cho rằng họ có thể tạo ra số lượng lớn các khóa mã ngẫu nhiên bằng cách đánh máy chữ một cách ngẫu nhiên. Tuy nhiên, mỗi lần thử, người đánh máy đều có xu hướng theo thói quen đánh máy một ký tự bằng tay trái rồi đến một ký tự bằng tay phải và như vậy là có sự luân chuyển giữa hai bên. Đây có thể là một cách tạo ra khóa mã một cách nhanh chóng song các dãy chữ cái lại có cấu trúc và không còn là ngẫu nhiên nữa - nếu người đánh máy đánh chữ cái **D**, ở bên trái của bàn phím, sau đó chữ cái tiếp theo có thể dự đoán được gần như sẽ là ở bên phải bàn phím. Nếu một khóa mã sổ tay dùng một lần thực sự là ngẫu nhiên thì tiếp theo một chữ cái bên trái bàn phím sẽ là một chữ cái cũng ở bên trái bàn phím với tỷ lệ khoảng gần một nửa.

Các nhà tạo mã cuối cùng cũng nhận ra rằng phải tốn rất nhiều thời gian, công sức và tiền bạc để tạo một khóa mã ngẫu nhiên. Những khóa mã ngẫu nhiên tốt nhất được tạo bởi những quá trình vật lý tự nhiên, chẳng hạn như sự phóng xạ, được biết là quá trình thực sự ngẫu nhiên. Các nhà tạo mã có thể đặt một mẫu chất phóng xạ trên một cái bàn và ghi sự phóng xạ của nó bằng máy đếm Geiger. Đôi khi sự phóng xạ tiếp nối nhau rất nhanh, đôi khi lại chậm lại - thời gian giữa hai phóng xạ là không thể dự đoán được và mang tính ngẫu nhiên. Các nhà tạo mã sau đó có thể nối một màn hình với máy đếm Geiger, trên đó quay vòng rất nhanh bảng chữ cái với tốc độ cố định, nhưng nó sẽ tạm thời ngưng lại mỗi khi ghi được một phóng xạ. Chữ cái nào lưu

trên màn hình sẽ được sử dụng làm chữ cái tiếp theo của khóa mã ngẫu nhiên. Rồi màn hình lại bắt đầu lại, nó quay vòng bảng chữ cái cho đến khi nó dừng lại một cách ngẫu nhiên do có một phóng xạ tiếp theo, chữ cái ngưng lại trên màn hình lại được bổ sung vào khóa mã và cứ tiếp tục như vậy. Sự sắp xếp này sẽ đảm bảo tạo nên một khóa mã thực sự ngẫu nhiên nhưng nó hoàn toàn phi thực tế đối với công việc mã hóa hằng ngày.

Ngay cả khi bạn có thể tạo ra đủ số khóa mã ngẫu nhiên thì vẫn còn một vấn đề thứ hai, đó là khó khăn trong việc phân phối chúng. Hãy thử hình dung cảnh tượng chiến trường, trong đó có hàng trăm điện báo viên cùng tham gia vào mạng lưới thông tin liên lạc. Trước tiên, mỗi người trong số họ phải có những mật mã sổ tay dùng một lần giống hệt nhau. Tiếp đó, khi những cuốn sổ tay mới được ban hành thì chúng cũng phải được phân phối đồng thời cho tất cả mọi người. Cuối cùng, tất cả phải tuân thủ quy trình để đảm bảo rằng họ sử dụng cùng trang sổ tay một lần vào cùng một thời điểm. Việc sử dụng sổ tay dùng một lần trên diện rộng như thế khiến chiến trường nhan nhản những người đưa và giữ sổ. Hơn nữa, nếu kẻ thù bắt được một bộ khóa mã thì toàn bộ hệ thống liên lạc sẽ bị tổn hại.

Có thể liều thử cắt giảm việc tạo và phân phối khóa mã bằng cách tái sử dụng các cuốn sổ tay dùng một lần, song đây lại là một sai lầm nghiêm trọng trong việc mã hóa. Tái sử dụng sổ tay một lần sẽ cho phép người phá mã của đối phương giải mã được các thư tín tương đối dễ dàng. Kỹ thuật được sử dụng để giải hai bản mật mã được mã hóa bằng cùng một khóa mã sổ tay dùng một lần sẽ được giải thích ở Phụ lục G, nhưng hiện thời, điểm quan trọng nhất lúc này đó là không có một cách sử dụng nhanh

gọn trong mật mã sổ tay dùng một lần. Người nhận và người gửi phải sử dụng khóa mã mới cho mỗi lần sử dụng.

Sổ tay dùng một lần trong thực tế chỉ được người ta sử dụng trong những liên lạc tối mật và có thể trang trải được những chi phí cực lớn trong việc tạo ra và phân phối khóa mã. Chẳng hạn, đường dây nóng giữa Tổng thống Nga và Tổng thống Mỹ được an toàn là nhờ sử dụng mật mã sổ tay dùng một lần.

Những điểm yếu trong thực tế của sổ tay dùng một lần, dù là hoàn hảo về mặt lý thuyết, đồng nghĩa với việc những ý tưởng của Mauborgne khó có thể được sử dụng ở thời điểm nóng bỏng của cuộc chiến. Trước hậu quả của Thế chiến Thứ nhất và toàn bộ sự thất bại của nó về mặt mật mã, cuộc tìm kiếm một hệ thống thực tế hơn để có thể sử dụng trong cuộc xung đột tiếp sau vẫn phải tiếp tục. Thật may mắn cho các nhà tạo mã, không bao lâu sau họ đã có một đột phá quan trọng, một thứ có thể thiết lập lại được sự an toàn trong mạng lưới thông tin liên lạc trên chiến trường. Để tăng sức mạnh cho mật mã của mình, các nhà tạo mã đã buộc phải từ bỏ phương pháp mã hóa bằng giấy bút mà sử dụng công nghệ tiên tiến nhất để mã hóa thông tin.

Sự phát triển của Máy mã - Từ Đĩa mã hóa đến máy Enigma

Máy mã hóa đầu tiên chính là đĩa mã hóa, được phát minh vào thế kỷ 15 bởi kiến trúc sư người Italia, Leon Alberti, một trong những cha đẻ của mật mã dùng một bảng chữ cái. Ông đặt hai chiếc đĩa bằng đồng, một chiếc nhỏ hơn chiếc kia một chút và khắc bảng chữ cái xung quanh mép của cả hai đĩa. Bằng cách đặt đĩa nhỏ hơn lên trên đĩa lớn hơn và cố định chúng bằng một cái

kim, có tác dụng như một trục, ông đã chế tạo ra một thứ tương tự như đĩa mã hóa ở Hình 31. Hai chiếc đĩa có thể quay một cách độc lập nên hai bảng chữ cái sẽ có vị trí tương đối khác nhau và nhờ vậy có thể sử dụng để mã hóa thông tin bằng dịch chuyển Caesar đơn giản. Chẳng hạn, để mã hóa thông tin với dịch chuyển Caesar một vị trí, vị trí của chữ **A** bên ngoài sẽ ở cạnh chữ **B** bên trong - đĩa bên ngoài là bảng chữ cái thường còn đĩa bên trong biểu thị bảng chữ cái mật mã. Mỗi chữ cái trong văn bản thường thì nhìn vào đĩa ngoài còn các chữ cái tương ứng trên đĩa bên trong được viết ra chính là của văn bản mật mã. Để mã hóa một bức thư với dịch chuyển Caesar năm vị trí, đơn giản là quay các đĩa sao cho chữ **A** bên ngoài nằm cạnh chữ **F** bên trong và sử dụng đĩa mã hóa ở vị trí mới của nó.

Mặc dù đĩa mã hóa là một thiết bị rất cơ bản song việc mã hóa lại đơn giản và nó đã được sử dụng trong suốt năm thế kỷ. Dạng đĩa mã hóa ở Hình 31 đã được sử dụng trong cuộc nội chiến ở Mỹ. Hình 32 trình bày máy Code-o-Graph, một đĩa mã hóa được sử dụng bởi nhân vật nổi tiếng trong vở *Thuyền trưởng Midnight*, một vở kịch truyền thanh thuở ban đầu của Mỹ. Người nghe có thể được sở hữu một máy Code-o-Graph bằng cách viết thư cho công ty tài trợ chương trình là Ovaltine kèm với nhãn hiệu của một trong những vỏ hộp sản phẩm của công ty này mà họ đã mua. Đôi khi chương trình sẽ kết thúc bằng một thông điệp mật mã từ Thuyền trưởng Midnight, để những người nghe trung thành giải mã bằng đĩa Code-o-Graph.

Đĩa mã hóa có thể được coi là một "máy mã", lấy mỗi chữ cái thường rồi biến đổi nó thành một thứ gì đó khác. Kiểu vận hành này đơn giản và mật mã đạt được cũng khá dễ bị hóa giải, nhưng

Hình 31 Đĩa mã hóa được sử dụng trong cuộc nội chiến ở nước My

đĩa mã hóa có thể sử dụng theo một cách phức tạp hơn. Người phát minh ra nó, Alberti, đã khuyến nghị thay đổi cách sắp đặt đĩa trong quá trình mã hóa, điều này tạo ra mật mã dùng nhiều bảng chữ cái chứ không phải một. Chẳng hạn, Alberti đã sử dụng đĩa để mã hóa từ **goodbye** với từ khóa mã là **LEON**. Ông bắt đầu bằng việc đặt đĩa theo chữ cái đầu của từ khóa mã, tức là dịch chuyển chữ **A** bên ngoài đến đứng cạnh chữ **L** bên trong. Sau đó ông mã hóa chữ cái đầu tiên của từ, tức chữ cái **g**, bằng cách tìm nó trên đĩa ngoài và ghi lại chữ cái tương ứng ở đĩa trong, là chữ **R**. Để mã hóa chữ cái thứ hai, ông điều chỉnh lại đĩa theo chữ cái thứ hai của từ khóa mã, sao cho chữ **A** bên ngoài đứng cạnh chữ **E** bên trong. Sau đó, ông mã hóa chữ **o** bằng cách tìm nó trên đĩa ngoài và ghi lại chữ cái tương ứng ở đĩa trong, là chữ **S**. Quá trình mã hóa tiếp tục với đĩa mã hóa được điều chỉnh theo chữ cái **O** của từ khóa mã, và tiếp theo là **N**, và sau đó trở lại **L** và cứ

Hình 32 Code-o-Graph của Thuyền trưởng Midnight, mã hóa mỗi chữ cái thường (đĩa ngoài) thành một con số (đĩa trong), chứ không phải thành một chữ cái.

tiếp tục như vậy. Alberti đã mã hóa thành công một thông tin bằng mật mã Vigenère với tên riêng của ông được sử dụng làm từ khóa mã. Đĩa mật mã làm tăng tốc độ mã hóa và giảm những sai sót so với hình thức mã hóa bằng hình vuông Vigenère.

Đặc điểm quan trọng của việc sử dụng đĩa mã hóa theo cách này đó là đĩa thay đổi cách thức mã hóa của nó trong quá trình mã hóa. Mặc dù độ phức tạp hơn này làm cho văn bản mật mã khó hóa giải hơn song cũng không phải là không giải được, vì chẳng qua là chúng ta dùng phiên bản cơ khí hóa của mật mã Vigenère mà thôi, mà mật mã Vigenère thì đã được giải mã bởi Babbage và Kasiski. Tuy nhiên, năm trăm năm sau Alberti, một dạng phức tạp hơn đã làm sống lại đĩa mã hóa của ông, và đã mang lại một thế hệ mật mã mới, thuộc hạng tầm cỡ khó hóa giải hơn bất kỳ loại mật mã nào đã sử dụng trước đây.

Năm 1918, nhà phát minh người Đức, Arthur Scherbius cùng người bạn thân là Richard Ritter đã thành lập một công ty mang tên Scherbius & Ritter, một hãng kỹ nghệ tân tiến làm đủ mọi thứ từ tuốcbin đến gối ngủ nhiệt. Scherbius chịu trách nhiệm nghiên cứu và phát triển, ông liên tục tìm kiếm những cơ hội mới. Một trong những dự án mà ông tâm đắc, đó là thay thế hệ thống mật mã sử dụng trong Thế chiến Thứ nhất đã không còn thích hợp nữa bằng cách chuyển việc mã hóa từ giấy bút sang một dạng mã hóa mới, sử dụng công nghệ thế kỷ 20. Nhờ học ngành kỹ thuật điện ở Hanover và Munich, ông đã phát minh ra một dạng máy mã hóa mà thực chất chính là đĩa mã hóa của Alberti thế hệ điện tử. Được gọi là Enigma, phát minh của Scherbius trở thành một hệ thống mã hóa đáng sợ nhất trong lịch sử.

Máy Enigma của Scherbius có chứa nhiều bộ phận tinh vi, kết hợp lại tạo thành một cỗ máy mã đồ sộ và phức tạp. Tuy nhiên, nếu chúng ta tháo tung cỗ máy này ra thành các bộ phận và rồi lắp ráp lại theo từng bước, thì những nguyên lý của nó sẽ trở nên dễ hiểu thôi. Dạng cơ bản phát minh của Scherbius gồm ba phần được nối với nhau bằng dây dẫn: một bàn phím để đánh vào các chữ cái thường, một bộ phận mã hóa dùng để mã hóa các chữ cái thường thành chữ cái mật mã tương ứng, và một bảng hiển thị chứa nhiều đèn để chỉ thị các chữ cái mật mã. Hình 33 trình bày một mặt cắt tiêu biểu của máy, và để đơn giản ta chỉ giới hạn xét bảng gồm sáu chữ cái. Để mã hóa một chữ cái trong văn bản thường, nhân viên mã hóa gõ vào chữ cái đó trên bàn phím, lập tức một xung điện được gửi tới bộ phận mã hóa trung tâm và đi ra phía bên kia, làm sáng chữ cái mật mã tương ứng trên bảng đèn.

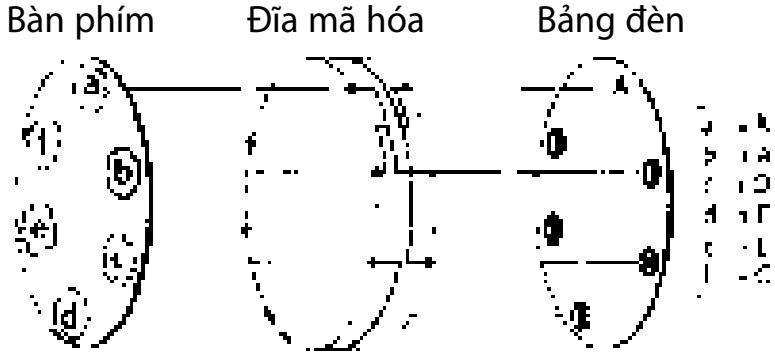
Bộ phận mã hóa, một chiếc đĩa cao su dày, chằng chịt dây dẫn, là bộ phận quan trọng nhất của máy. Từ bàn phím, các dây dẫn đi vào bộ phận mã hóa ở sáu điểm, sau đó qua một loạt những uốn lượn rắc rối trong bộ phận mã hóa trước khi đi ra ở sáu điểm, phía bên kia. Việc nối dây bên trong bộ phận mã hóa sẽ quyết định các chữ cái thường bị mã hóa như thế nào. Chẳng hạn, ở Hình 33, các dây dẫn quyết định rằng:

đánh chữ **a** sẽ làm sáng đèn chữ **B**, tức là **a** được mã hóa thành **B**;
đánh chữ **b** sẽ làm sáng đèn chữ **A**, tức là **b** được mã hóa thành **A**;
đánh chữ **c** sẽ làm sáng đèn chữ **D**, tức là **c** được mã hóa thành **D**;
đánh chữ **d** sẽ làm sáng đèn chữ **F**, tức là **d** được mã hóa thành **F**;
đánh chữ **e** sẽ làm sáng đèn chữ **E**, tức là **e** được mã hóa thành **E**;
đánh chữ **f** sẽ làm sáng đèn chữ **C**, tức là **f** được mã hóa thành **C**;

Từ **cafe** khi đó sẽ được mã hóa thành **DBCE**. Với cách cài đặt cơ bản này thì bộ phận mã hóa thực chất là xác định bảng chữ cái mật mã và máy có thể được sử dụng để thực hiện một mật mã thay thế dùng một bảng chữ cái đơn giản.

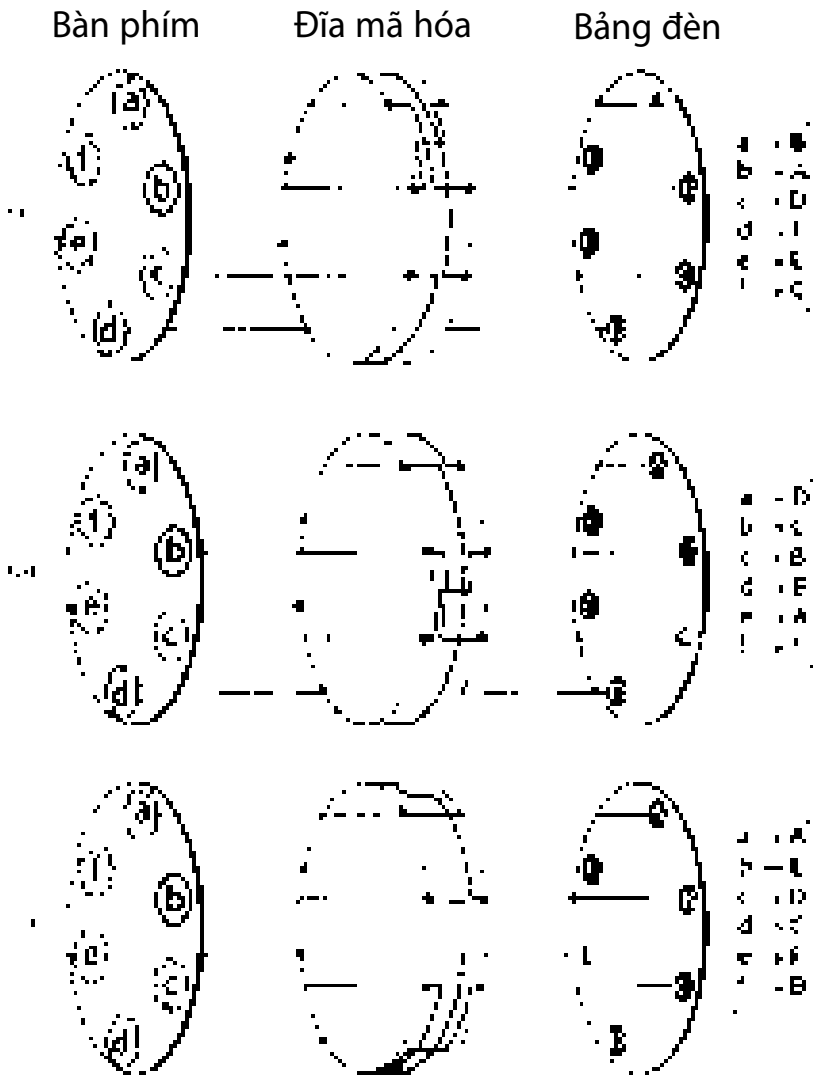
Tuy nhiên, ý tưởng của Scherbius là để cho đĩa mã hóa tự động quay 1/6 vòng mỗi khi một chữ cái được mã hóa (hay 1/26 vòng đối với một bảng chữ cái đủ 26 chữ cái). Hình 34 (a) trình bày cách sắp đặt như ở Hình 33; lại một lần nữa, khi đánh chữ cái **b** sẽ làm sáng đèn ở chữ cái **A**. Tuy nhiên lần này, ngay sau khi đánh một chữ cái và làm sáng đèn ở bảng đèn, đĩa mã hóa quay 1/6 vòng đến vị trí như ở Hình 34(b). Lúc này đánh chữ cái **b** lần nữa sẽ làm sáng đèn một chữ cái khác, đó là **C**. Ngay sau đó, đĩa mã hóa lại quay đến vị trí ở Hình 34(c). Lúc này, đánh chữ cái **b**

sẽ làm sáng đèn ở chữ cái **E**. Đánh chữ cái **b** sáu lần liên tiếp sẽ tạo ra bản mật mã là **ACEBDC**. Nói cách khác, bảng chữ cái mật mã thay đổi sau mỗi lần mã hóa và việc mã hóa chữ cái **b** cũng thay đổi liên tục. Với việc cho quay như vậy, đĩa mã hóa thực chất là xác định 6 bảng chữ cái và máy có thể được sử dụng để thực hiện mật mã dùng nhiều bảng chữ cái.



Hình 33 Một phiên bản đơn giản hóa của máy Enigma với bảng chữ cái chỉ gồm sáu chữ cái. Bộ phận quan trọng nhất của máy là đĩa mã hóa. Bằng việc đánh vào chữ cái **b** trên bàn phím, một dòng điện đi vào đĩa mã hóa, theo đường nối dây bên trong và sau đó đi ra và làm sáng đèn **A**. Nói gọn lại, **b** được mã hóa thành **A**. Hình chữ nhật nhỏ ở bên phải biểu thị mỗi chữ cái được mã hóa như thế nào.

Sự quay của đĩa mã hóa là đặc điểm quan trọng nhất trong thiết kế của Scherbius. Tuy nhiên, nếu chỉ như thế thì máy này vẫn có một điểm yếu rõ rệt. Sau khi đánh chữ cái **b** sáu lần, đĩa mã hóa lại trở về vị trí ban đầu và tiếp tục đánh chữ **b** nhiều lần nữa thì sẽ lặp lại hình mẫu mã hóa. Nói chung, những người tạo mã cố tránh sự lặp lại vì nó sẽ dẫn tới tính quy luật và cấu trúc trong văn bản mật mã, những triệu chứng của một loại mật mã yếu. Vấn đề này có thể hạn chế bằng cách thêm vào đĩa mã hóa thứ hai.



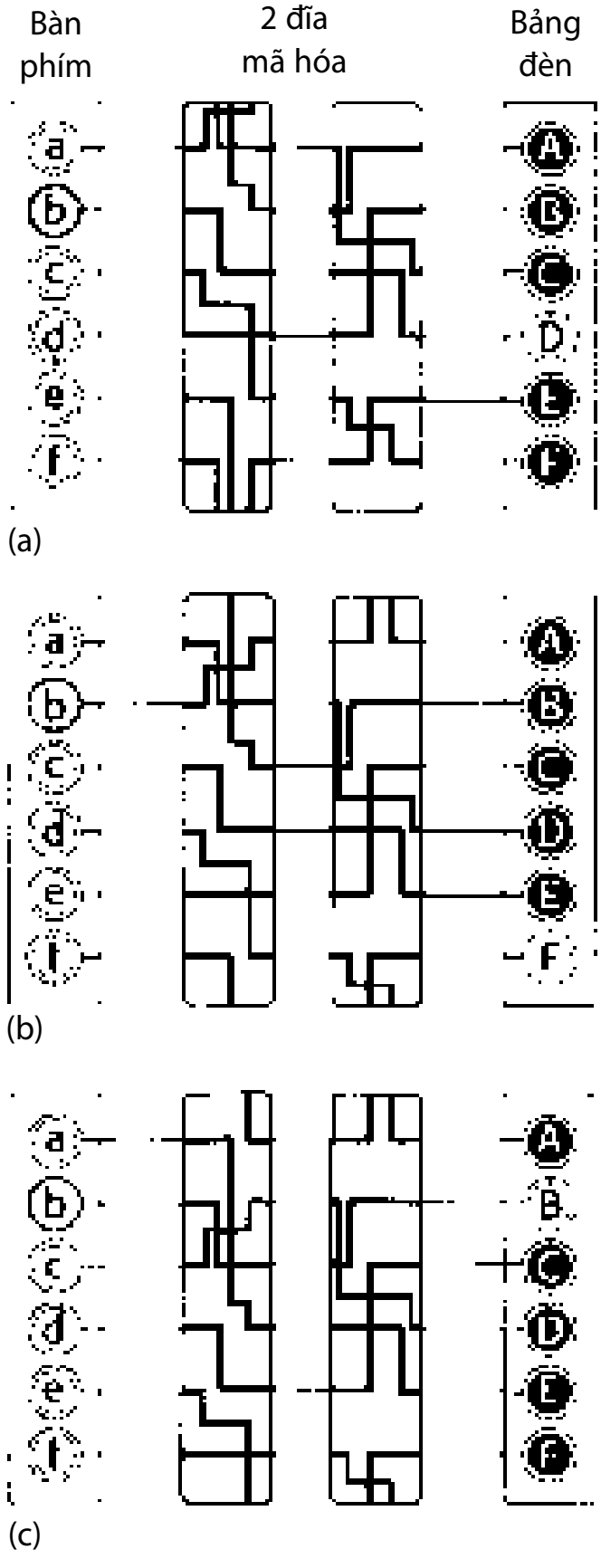
Hình 34 Mỗi lần một chữ cái được đánh từ bàn phím và được mã hóa, đĩa mã hóa lại quay đến một vị trí khác, làm thay đổi cách mã hóa mỗi chữ cái. Ở (a), đĩa mã hóa mã hóa **b** thành **A**, nhưng ở (b) vị trí mới của đĩa mã hóa lại mã hóa **b** thành **C**. Ở (c), sau khi quay thêm một vị trí nữa, đĩa mã hóa lại mã hóa **b** thành **E**. Sau khi mã hóa bốn chữ cái nữa và quay bốn vị trí nữa, đĩa mã hóa quay trở về vị trí ban đầu.

Hình 35 là một mô hình máy mã với hai đĩa mã hóa. Vì rất khó vẽ đĩa mã hóa ba chiều với các đường nối dây ba chiều bên trong nên Hình 35 chỉ trình bày biểu diễn ở không gian hai chiều. Mỗi lần một chữ cái được mã hóa, đĩa mã hóa thứ nhất quay đi một vị trí hay trong sơ đồ không gian hai chiều, mỗi dây dẫn

dịch xuống một vị trí. Ngược lại, đĩa mã hóa thứ hai vẫn đứng yên hầu hết thời gian. Nó chỉ quay sau khi đĩa thứ nhất đã hoàn tất một vòng. Đĩa thứ nhất được gắn một cái răng và chỉ khi cái răng này chạm tới một điểm nhất định, nó sẽ đẩy đĩa mã hóa thứ hai tiến một vị trí.

Trong Hình 35(a), đĩa mã hóa thứ nhất đang ở vị trí chuẩn bị đẩy đĩa mã hóa thứ hai dịch chuyển. Việc đánh vào và mã hóa một chữ cái sẽ làm dịch chuyển các đĩa mã hóa đến cấu hình như trên Hình 35(b), trong đó đĩa mã hóa thứ nhất đã dịch đi một vị trí và đĩa mã hóa thứ hai cũng bị đẩy đi một vị trí. Việc đánh vào và mã hóa một chữ cái khác làm dịch đĩa mã hóa thứ nhất đi một vị trí, Hình 35(c), nhưng lần này thì đĩa mã hóa thứ hai vẫn đứng yên. Đĩa mã hóa thứ hai sẽ không dịch chuyển cho đến khi đĩa mã hóa thứ nhất hoàn tất một vòng quay, tức là sau năm lần mã hóa nữa. Sự vận hành như thế này cũng tương tự như đồng hồ đo quãng đường ở xe hơi - rôto hiển thị số dặm hàng đơn vị thì quay rất nhanh và khi nó quay một vòng đạt đến số "9", nó sẽ đẩy rôto hiển thị số dặm hàng chục quay đi một vị trí.

Lợi thế của việc bổ sung thêm một đĩa mã hóa là cách mã hóa sẽ không lặp lại cho đến khi đĩa mã hóa thứ hai trở lại vị trí ban đầu của nó, tức là sau sáu vòng quay của đĩa thứ nhất, hay sau khi $6 \times 6 = 36$ chữ cái được mã hóa. Nói cách khác, có 36 cách kết hợp khác nhau của hai đĩa mã hóa, tương đương với việc chuyển đổi giữa 36 bảng chữ cái mật mã. Với bảng chữ cái đầy đủ gồm 26 chữ cái thì máy mã hóa sẽ chuyển đổi giữa $26 \times 26 = 676$ bảng chữ cái mật mã. Như vậy bằng cách kết hợp các đĩa mã hóa (đôi khi còn gọi là rôto), có thể tạo ra một máy mã hóa chuyển đổi liên tục giữa các bảng chữ cái khác nhau.



Hình 35 Nhờ có thêm đĩa mã hóa thứ hai, hình mẫu mã hóa không lặp lại cho đến khi 36 chữ cái được mã hóa, tại đó cả hai đĩa mã hóa đều trở về vị trí ban đầu. Để đơn giản hóa sơ đồ, hai đĩa mã hóa được biểu diễn ở không gian hai chiều; thay vì quay đi một vị trí, các đường nối dây sẽ dịch xuống một vị trí. Nếu một dây dẫn xuất phát từ đỉnh hay đáy của một đĩa mã hóa thì đường đi của nó sẽ được nối tiếp vào dây dẫn tương ứng ở đáy hay đỉnh của chính đĩa mã hóa đó. Ở (a), **b** được mã hóa thành **D**. Sau khi mã hóa, đĩa mã hóa thứ nhất quay đi một vị trí, đồng thời đẩy đĩa mã hóa thứ hai quay đi một vị trí - điều này chỉ xảy ra duy nhất một lần trong suốt một vòng quay của đĩa thứ nhất. Vị trí mới này được biểu thị ở (b), trong đó **b** được mã hóa thành **F**. Sau khi mã hóa, đĩa thứ nhất quay một vị trí nhưng lần này đĩa thứ hai vẫn đứng yên. Vị trí mới này được thể hiện ở (c), trong đó **b** được mã hóa thành **B.**

Người mã hóa đánh vào một chữ cái nào đó và tùy thuộc vào sự sắp đặt của hai đĩa mã hóa, nó có thể được mã hóa theo một trong hàng trăm bảng chữ cái mật mã. Sau đó, sự sắp đặt này lại thay đổi, vì vậy khi chữ cái thứ hai được đánh vào máy thì nó lại được mã hóa theo một bảng chữ cái mật mã khác. Hơn nữa, tất cả những điều đó được thực hiện với hiệu quả cao và rất chính xác, nhờ sự chuyển động tự động của đĩa mã hóa và tốc độ của dòng điện.

Trước khi giải thích chi tiết Scherbius dự định sử dụng máy mã hóa của mình như thế nào, cần phải mô tả thêm hai yếu tố nữa trong máy Enigma, được trình bày ở Hình 36. Trước hết, máy mã hóa chuẩn của Scherbius còn sử dụng thêm một đĩa mã hóa thứ ba để tăng thêm độ phức tạp - đối với một bảng chữ cái đầy đủ thì ba đĩa mã hóa này sẽ cho $26 \times 26 \times 26 = 17.576$ cách sắp đặt khác nhau giữa ba đĩa mã hóa. Thứ hai là, Scherbius bổ sung thêm một bộ phận gọi là *đĩa phản xạ* (reflector). Đĩa phản xạ phần nào cũng giống như đĩa mã hóa, ở chỗ nó cũng là một đĩa cao su với rất nhiều đường nối dây bên trong, song khác ở chỗ là nó không quay và các dây dẫn đi vào và sau đó đi ra từ cùng một phía. Với việc lắp đặt thêm đĩa phản xạ, khi nhân viên mã hóa đánh vào một chữ cái, nó sẽ gửi đi một tín hiệu điện qua ba đĩa mã hóa. Khi đĩa phản xạ nhận được tín hiệu tới, nó sẽ gửi trở lại qua ba đĩa mã hóa ban đầu nhưng bằng con đường khác. Chẳng hạn, với cách sắp đặt như Hình 36, khi đánh chữ cái **b** sẽ gửi một tín hiệu qua ba đĩa mã hóa và đi vào đĩa phản xạ, tại đây tín hiệu sẽ truyền trở lại qua các dây dẫn đến chữ cái **D**. Thực tế thì tín hiệu không đi qua bàn phím như chúng ta có cảm tưởng như thế khi nhìn Hình 36, mà nó dẫn thẳng tới bảng đèn. Thoạt

trông thì đĩa phản xạ dường như thêm vào máy cũng chẳng có ích lợi gì, vì bản chất cố định của nó đồng nghĩa với việc nó không bổ sung thêm số bảng chữ cái mật mã nào. Tuy nhiên, lợi ích của nó sẽ trở nên rõ ràng khi chúng ta xem máy thực sự được sử dụng để mã hóa và giải mã thông tin như thế nào.

Một người muốn gửi đi một bức thư bí mật. Trước khi việc mã hóa bắt đầu, người này phải quay các đĩa mã hóa đến một vị trí khởi động nhất định. Có 17.576 cách sắp đặt có thể và vì vậy có 17.576 vị trí xuất phát khả dĩ. Sự thiết đặt ban đầu các đĩa mã hóa sẽ quyết định bức thư sẽ được mã hóa như thế nào. Chúng ta có thể hình dung máy Enigma qua hệ thống mã hóa tổng quát, và cách sắp đặt ban đầu sẽ quyết định các chi tiết chính xác của việc mã hóa. Nói cách khác, cách sắp đặt đầu tiên sẽ cung cấp cho ta khóa mã. Cách sắp đặt đầu tiên thường được quy định từ sổ mã, trong đó liệt kê khóa mã cho mỗi ngày và luôn có sẵn cho tất cả những ai tham gia vào hệ thống thông tin liên lạc. Việc phân phối sổ mã đòi hỏi phải có thời gian và sức lực, song vì chỉ có một khóa mã dùng cho một ngày nên có thể chỉ cần gửi đi một sổ mã có chứa 28 khóa mã, bốn tuần một lần. Đem so sánh, nếu quân đội sử dụng mật mã sổ tay dùng một lần thì cứ mỗi bức thư lại cần một khóa mã mới, vì vậy việc phân phối khóa mã sẽ là một nhiệm vụ khó khăn hơn nhiều. Một khi các đĩa mã hóa được thiết đặt theo yêu cầu hằng ngày trong sổ mã, người gửi có thể bắt đầu tiến hành mã hóa. Người này đánh vào chữ cái đầu tiên của bức thư, xem chữ cái nào xuất hiện trên bảng đèn và ghi lại nó, đó chính là chữ cái đầu tiên trong văn bản mật mã. Sau đó, đĩa mã hóa thứ nhất tự động quay đi một vị trí, người gửi đánh vào chữ cái thứ hai và tiếp tục như vậy. Khi anh ta đã hoàn thành

xong văn bản mật mã, chuyển nó cho điện báo viên và người này sẽ truyền bức thư đến người nhận định trước.

Để giải mã bức thư, người nhận cần phải có máy Enigma và một bản sổ mã có chứa cách sắp đặt đầu tiên cho ngày hôm đó. Anh ta đặt máy theo sổ mã, đánh vào từng chữ cái mật mã và bảng đèn sẽ hiển thị chữ cái thường. Nói cách khác, người gửi đánh vào chữ cái thường để tạo ra chữ cái mật mã, còn người nhận đánh vào chữ cái mật mã để ra chữ cái thường - văn bản mật mã và văn bản giải mã như là một quá trình phản chiếu qua gương. Sự đơn giản trong việc giải mã chính là nhờ ở đĩa phản xạ. Từ Hình 36, ta có thể thấy nếu chúng ta đánh vào chữ **b** và theo đường dẫn, chúng ta trở lại chữ **D**. Tương tự, nếu ta đánh vào chữ **d** và theo đường dẫn, thì chúng ta trở lại chữ **B**. Máy mã hóa chữ cái thường thành chữ cái mật mã và chừng nào máy vẫn thiết đặt ở chế độ như nhau thì nó sẽ chuyển chữ cái mật mã đó trở lại thành chữ cái thường tương ứng.

Hiển nhiên là khóa mã, và sổ mã có chứa khóa đó, không bao giờ được để lọt vào tay kẻ thù. Hoàn toàn có khả năng là kẻ thù bắt được một chiếc máy Enigma song khi không biết cách sắp đặt đầu tiên được sử dụng để mã hóa thì họ không thể giải mã bức thư bắt được một cách dễ dàng. Không có sổ mã, những nhà giải mã của đối phương phải sử dụng biện pháp là thử tất cả các khóa mã có thể, tức là thử tất cả 17.576 cách sắp đặt đầu tiên khả dĩ. Nhà giải mã tuyệt vọng này sẽ thử đặt máy Enigma họ bắt được ở một vị trí nào đó, đánh vào một đoạn ngắn của văn bản mật mã và xem thử các chữ cái hiện ra có mang ý nghĩa nào đó không. Nếu không, anh ta sẽ thay đổi cách sắp đặt khác và thử lại lần nữa. Nếu để thử một cách sắp đặt mất một phút và

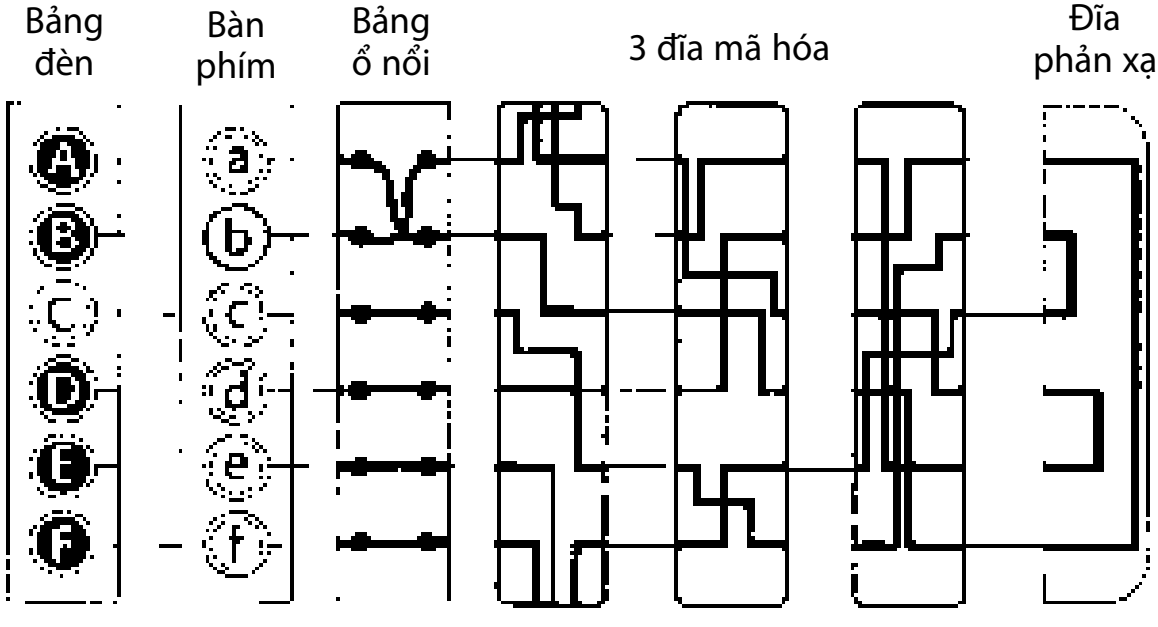
làm việc cả ngày lẫn đêm thì sẽ phải mất khoảng hai tuần mới thử hết tất cả các cách sắp đặt. Đây mới chỉ là mức độ an toàn trung bình, song nếu đối phương cử mười hai người làm nhiệm vụ này thì tất cả các cách sắp đặt có thể thử trong vòng một ngày. Vì vậy, Scherbius quyết định cải thiện mức độ an toàn cho phát minh của mình bằng cách tăng thêm số cách sắp đặt ban đầu và nhờ đó làm tăng số khóa mã tiềm năng.

Ông đã làm tăng độ an toàn bằng cách bổ sung thêm đĩa mã hóa (mỗi đĩa mã hóa sẽ làm tăng số khóa mã lên 26 lần), nhưng như thế thì sẽ làm cho máy Enigma trở nên quá cồng kềnh. Thay vì làm vậy, ông bổ sung thêm hai đặc điểm khác nữa. Một là chỉ đơn giản làm cho các đĩa mã hóa có thể di chuyển được và có thể đổi chỗ cho nhau. Như vậy thì, chẳng hạn, đĩa thứ nhất có thể di chuyển tới vị trí thứ ba và đĩa thứ ba chuyển đến vị trí thứ nhất. Sự sắp xếp của các đĩa mã hóa có ảnh hưởng tới việc mã hóa nên vị trí chính xác là rất quan trọng đối với việc mã hóa và giải mã. Có sáu cách sắp xếp khác nhau giữa ba đĩa mã hóa và đặc điểm này làm tăng số khóa mã, hay số các cách sắp đặt ban đầu lên sáu lần.

Đặc điểm mới thứ hai được thêm vào là một *bảng ổ nối* nằm giữa bàn phím và đĩa mã hóa thứ nhất. Bảng ổ nối cho phép người gửi nối thêm vào các dây cáp có tác dụng hoán đổi một số chữ cái trước khi đi qua đĩa mã hóa. Ví dụ, một dây cáp có thể được sử dụng để nối ổ **a** với **b** trên bảng ổ nối, nhờ vậy khi người mã hóa muốn mã hóa chữ cái **b**, tín hiệu điện sẽ đi theo con đường đến các đĩa mã hóa mà lẽ ra là đường đi của chữ cái **a** và ngược lại. Người sử dụng Enigma có sáu dây cáp, tức là có sáu cặp chữ cái có thể được hoán đổi, còn lại mười bốn chữ cái không được

nối và không hoán đổi được cho nhau. Các chữ cái được hoán đổi bằng bảng ổ nối là một phần của sự sắp đặt ban đầu của máy và vì vậy phải được ghi trong sổ mã. Hình 37 cho thấy sự bố trí của máy có cả bảng ổ nối. Vì sơ đồ chỉ xử lý bảng chữ cái gồm sáu chữ cái nên chỉ có một cặp chữ cái là **a** và **b** đã được hoán đổi.

Còn có một đặc điểm nữa trong thiết kế của Scherbius, được gọi là *vòng* (ring) mà ta còn chưa đề cập đến. Mặc dù vòng cũng có ảnh hưởng nhất định đến việc mã hóa, song nó là một bộ phận ít quan trọng nhất trong cả cỗ máy Enigma, nên tôi quyết định bỏ qua vì mục đích của phần này. (Bạn đọc nào muốn biết về vai trò chính xác của vòng có thể tham khảo một số cuốn sách trong danh mục sách cần đọc thêm, chẳng hạn như cuốn *Tìm*



Hình 37 Bảng ổ nối nằm giữa bàn phím và đĩa mã hóa thứ nhất. Bằng cách nối các dây cáp, nó có thể hoán đổi một cặp chữ cái, nhờ vậy, ở ví dụ này, **b** được hoán đổi với **a**. Giờ, **b** được mã hóa theo con đường mà trước đó dùng để mã hóa **a**. Trong máy Enigma thực sự với 26 chữ cái, người ta sử dụng sáu dây cáp để hoán đổi sáu cặp chữ cái.

hiểu Enigma của David Kahn. Danh mục này cũng giới thiệu hai trang Web có chứa những mô hình Enigma rất tuyệt để bạn có thể thử vận hành một máy Enigma thực thụ).

Giờ thì chúng ta đã biết tất cả những bộ phận chính của máy Enigma của Scherbius. Có thể tính ra số khóa mã bằng cách tổ hợp số các dây cáp trên bảng ổ nối với số cách sắp đặt và định hướng của các đĩa mã hóa. Danh sách dưới đây cho thấy mỗi biến số của máy và số các khả năng tương ứng với mỗi biến số đó:

Định hướng của đĩa mã hóa. Mỗi đĩa trong ba đĩa mã hóa có thể được đặt ở một trong 26 định hướng. Như vậy sẽ có 26 × 26 × 26 cách sắp đặt: 15.576

Cách sắp đặt các đĩa mã hóa. Ba đĩa mã hóa (1, 2 và 3) có thể sắp đặt theo một trong sáu trật tự sau: 123, 132, 213, 231, 312, 321 6

Bảng ổ nối. Số cách kết nối để hoán đổi 6 cặp chữ cái trong số 26 chữ cái là cực kỳ lớn: 100.391.791.500

Tổng cộng. Số khóa mã là tích của ba số trên:

17.576 × 6 × 100.391.791.500

= 10.000.000.000.000.000

Chừng nào người gửi và người nhận đã thỏa thuận với nhau về cách nối cáp trong bảng ổ nối, về trật tự các đĩa mã hóa và sự định hướng tương ứng của chúng, tức là tất cả các thông số xác định khóa mã, thì họ có thể mã hóa và giải mã một cách dễ dàng. Tuy nhiên, với đối phương không biết khóa mã, họ sẽ phải thử từng khóa mã khả dĩ trong số 10.000.000.000.000.000 để giải mã. Để dễ hình dung, một nhà giải mã kiên trì nhất, có thể thử mỗi một khả năng trong một phút, sẽ phải mất khoảng

thời gian dài hơn cả tuổi của vũ trụ để thử tất cả các khả năng. (Vì tôi đã bỏ qua tác dụng của các vòng trong những tính toán ở trên, chứ thực ra số khóa mã có thể thậm chí còn lớn hơn và thời gian hóa giải Enigma cũng sẽ lâu hơn).

Arthur Scherbius

Vì cho đến lúc này, đóng góp vào số khóa mã lớn nhất là từ bảng ổ nối, nên bạn có thể ngạc nhiên tự hỏi tại sao Scherbius lại vẫn cứ băn khoăn trăn trở với các đĩa mã hóa. Đứng riêng một mình, bảng ổ nối chỉ cung cấp một mật mã tầm thường, không hơn gì mật mã thay thế dùng một bảng chữ cái, hoán đổi chỉ trong vòng 12 chữ cái. Vấn đề đặt ra với bảng ổ nối, đó là sự hoán đổi sẽ không thay đổi một khi việc mã hóa được bắt đầu, vì đứng riêng ra, nó chỉ tạo ra một văn bản mật mã dễ dàng giải mã được bằng phương pháp phân tích tần suất. Các đĩa mã hóa đóng góp số lượng khóa mã ít hơn, song sự sắp đặt của nó thay đổi liên lục, đồng nghĩa với việc văn bản mật mã thu được không thể hóa giải bằng kỹ thuật phân tích tần suất. Bằng cách kết hợp các đĩa mã hóa với bảng ổ nối, Scherbius đã làm cho máy của mình chống lại được phép phân tích tần suất, và đồng thời cũng mang lại cho nó một số lượng khóa mã khổng lồ.

Scherbius đã nhận được bằng phát minh sáng chế vào năm 1918. Máy mã hóa của ông được đựng trong hộp nhỏ với kích thước chỉ cỡ 34 × 28 × 15 cm, song lại nặng tới 12 kg. Hình 39

là một chiếc máy Enigma với nắp ngoài mở, sẵn sàng để sử dụng. Ta có thể nhìn thấy bàn phím dùng để đánh vào các chữ cái của văn bản thường và bên trên nó là bảng đèn nơi hiện lên các chữ cái mật mã. Phía dưới bàn phím là bảng ổ nối; có hơn sáu cặp chữ cái được hoán đổi nhờ bảng ổ nối này, vì máy Enigma này là thế hệ sau, đã được cải tiến đôi chút so với thiết kế ban đầu mà tôi vừa mô tả ở trên. Hình 40 là một máy Enigma với nắp bên trong mở, để lộ thêm các chi tiết mà đặc biệt là ba đĩa mã hóa.

Scherbius tin rằng máy Enigma là không thể bị đánh bại và sức mạnh mã hóa của nó sẽ tạo ra sức tiêu thụ rất lớn. Ông đã

Hình 39 Máy Enigma quân sự sẵn sàng hoạt động

thử tiếp thị Enigma đến cả cộng đồng doanh nghiệp lẫn quân đội, với thiết kế thích hợp cho mỗi đối tượng. Chẳng hạn, ông đã giới thiệu hệ máy Enigma cơ bản cho giới doanh nghiệp, còn phiên bản ngoại giao sang trọng cho Bộ Ngoại giao còn kèm thêm cả một máy in chứ không phải là bảng đèn. Giá cả của mỗi máy tương đương với khoảng 30.000 đôla theo mức giá hiện nay.

Thật không may là giá quá cao của máy đã làm e ngại nhiều khách hàng tiềm năng. Giới kinh doanh thì cho rằng họ không đủ tiền bạc để trang trải cho sự an toàn của Enigma, còn Scherbius thì cho rằng họ không có đủ tiền bạc là do không có nó. Ông đưa

Hình 40 Máy Enigma với nắp bên trong mở, để lộ ba đĩa mã hóa

ra lý lẽ rằng một bức thư quan trọng sống còn bị bắt được bởi đối thủ cạnh tranh có khi còn làm cho công ty mất cả cơ nghiệp, nhưng chẳng mấy doanh nhân đếm xỉa tới lời ông nói. Quân đội Đức cũng không mấy mặn mà, vì họ đã lãng quên những thiệt hại do mật mã không an toàn của mình gây ra trong Thế chiến Thứ nhất. Chẳng hạn, họ đã bị lừa để tin rằng bức điện tín Zimmermann đã bị điệp viên Mỹ đánh cắp ở Mexico và vì vậy họ cho rằng sai lầm là ở chỗ an ninh của Mexico. Họ vẫn không hề ý thức được rằng bức điện trong thực tế đã bị Anh chặn bắt được và giải mã, và rằng sự thất bại của Zimmermann chính là sự thất bại của mật mã Đức.

Tuy nhiên, không chỉ một mình Scherbius phải chịu sự vỡ mộng một cách đơn độc. Ba nhà phát minh độc lập ở ba nước khác cũng gần như đồng thời nảy ra ý tưởng về một máy mật mã dựa trên các đĩa mã hóa quay. Tại Hà Lan năm 1919, Alexander Koch đã được cấp bằng phát minh số 10.700, song ông cũng thất bại trong việc thương mại hóa phát minh của mình và cuối cùng đã bán bản quyền vào năm 1927. Tại Thụy Điển, Arvid Damm cũng nhận bằng phát minh tương tự, nhưng cho đến tận khi qua đời vào năm 1927 ông vẫn không sao tìm được thị trường. Tại Mỹ, nhà phát minh Edward Hebern cũng đã rất tin tưởng vào phát minh của mình, được gọi là Nhân sư Vô tuyến, nhưng thất bại của ông lại là nặng nề nhất.

Vào giữa những năm 1920, Hebern bắt đầu xây dựng một nhà máy trị giá 380.000 đôla, song không may cho ông, lúc đó là thời kỳ Mỹ đang chuyển đổi từ trạng thái đa nghi sang cởi mở. Thập kỷ trước, do hậu quả của Thế chiến Thứ nhất, Chính phủ Hoa Kỳ đã lập ra Phòng Đen, một cơ quan mật mã rất hiệu quả

với đội ngũ nhân viên gồm hai mươi nhà giải mã, dưới sự lãnh đạo của một người đàn ông xuất sắc nhưng hơi phô trương tên là Herbert Yardley. Sau này, Yardley đã từng viết "Phòng Đen, được khóa chặt, kín đáo, được bảo vệ chặt chẽ, nhưng nhìn và nghe thấy hết. Mặc dù những tấm màn được kéo kín và các cửa sổ được che rèm rất dày song tai mắt tầm xa của nó có thể xâm nhập vào những căn phòng họp bí mật ở Washington, Tokyo, London, Paris, Geneva, Rôma. Những đôi tai nhạy cảm của nó có thể bắt được những tiếng thì thầm yếu ớt nhất ở thủ đô các nước trên thế giới." Phòng Đen của Mỹ đã xử lý 45.000 bức điện mã hóa trong một thập kỷ, song cho đến khi Hebern xây dựng nhà máy của mình thì Herbert Hoover trúng cử Tổng thống và mong muốn mở ra một thời đại mới của lòng tin trong các vấn đề quốc tế. Ông đã xóa bỏ Phòng Đen và Ngoại trưởng của ông, Henry Stimson, tuyên bố "Người lịch sự không đọc thư từ của người khác". Nếu một quốc gia cho rằng đọc thư của người khác là sai thì nó cũng bắt đầu tin rằng người khác không đọc thư từ của chính nó, và vì vậy không thấy cần thiết phải quan tâm đến các máy mật mã. Hebern chỉ bán được có 12 máy với tổng số tiền khoảng 1.200 đôla và năm 1926, ông đã bị đưa ra tòa vì không thanh toán sòng phẳng cho các cổ đông và bị tuyên phạt theo Luật Chứng khoán Công ty của bang California.

Tuy nhiên, may mắn thay cho Scherbius, giới quân sự Đức cuối cùng đã bị buộc phải đánh giá lại giá trị của máy Enigma, nhờ các tài liệu của hai người Anh. Một là cuốn *Khủng hoảng Thế giới* của Winston Churchill xuất bản năm 1923, trong đó có đề cập đến việc người Anh đã tiếp cận được với tài liệu mã hóa của người Đức như thế nào:

> Vào đầu tháng Chín năm 1914, một chiến hạm hạng nhẹ của Đức tên là Magdeburg, bị đắm ở vùng biển Baltic. Xác của một hạ sĩ quan Đức bị chết đuối đã được người Nga vớt lên sau đó vài giờ và trong ngực ông ta được giữ chặt bởi cánh tay đã chết cứng là cuốn sách tín hiệu và mật mã của hải quân Đức và các tấm bản đồ Biển Bắc và Vịnh Heligoland được kẻ ô vuông rất chi tiết. Ngày 6 tháng Chín, Tùy viên Hải quân Nga đã đến gặp tôi. Ông ta đã nhận được một bức thư từ Petrograd kể về những gì đã xảy ra và Bộ Hải quân Nga với sự hỗ trợ của các cuốn sách tín hiệu và mật mã thu được có thể giải mã được ít nhất là các thư từ của Hải quân Đức. Người Nga thấy rằng với vai trò dẫn đầu về sức mạnh hải quân, Bộ Hải quân Anh cần có các cuốn sách và bản đồ đó. Nếu chúng tôi gửi công hàm tới cho Alexandrov thì các sĩ quan Nga chịu trách nhiệm về những cuốn sách này sẽ gửi chúng đến Anh.

Tài liệu này đã giúp các nhà giải mã của Phòng 40 hóa giải được các bức thư mã hóa một cách thông thường của quân Đức. Cuối cùng, gần một thập kỷ sau, người Đức mới ý thức được sự thất bại đó trong an ninh thông tin liên lạc của mình. Cũng vào năm 1923, Hải quân Hoàng gia Anh đã công bố lịch sử chính thức của họ trong Thế chiến Thứ nhất, trong đó có nhắc lại sự thật về việc chặn bắt và giải mã thông tin của quân Đức đã mang lại một lợi thế rõ ràng cho quân Đồng minh. Thành tựu đáng tự hào này của Tình báo Anh là một sự phán xét không thể chối cãi đối với những người chịu trách nhiệm về an ninh Đức, những người sau đó đã phải thừa nhận trong báo cáo của mình rằng "Chỉ huy hạm đội Đức, mà thư từ qua sóng vô tuyến của họ đã bị quân Anh bắt được và giải mã, đã chơi một ván bài ngửa với chỉ huy hải quân Anh."

Giới quân sự Đức buộc phải đòi hỏi làm thế nào đó để tránh không lặp lại thất bại thảm hại trong lĩnh vực mật mã như trong Thế chiến Thứ nhất và đã đưa ra kết luận rằng máy Enigma là lựa chọn tốt nhất. Vào năm 1925, Scherbius bắt đầu cho sản xuất hàng loạt máy Enigma để đưa ra phục vụ cho quân đội vào năm sau và tiếp đó nó được chính phủ và một số tổ chức nhà nước, như các công ty hỏa xa sử dụng. Những máy Enigma này khác với một số máy mà Scherbius trước đây đã bán cho các doanh nghiệp, vì các đĩa mã hóa có những đường nối dây khác ở bên trong. Vì vậy mà những người có máy Enigma thương mại không biết được đầy đủ về những máy dùng cho quân đội và cho chính phủ.

Trong hai thập kỷ sau đó, quân đội Đức đã mua 30.000 máy Enigma. Phát minh của Scherbius đã cung cấp cho quân đội Đức một hệ thống mã hóa an toàn nhất thế giới và khi nổ ra Thế chiến Thứ hai, thông tin liên lạc của họ được bảo vệ bởi một trình độ mã hóa vô song. Đôi lúc tưởng như máy Enigma đã có một vai trò sống còn trong việc bảo đảm chiến thắng cho Đức quốc xã, song thay vì thế, cuối cùng nó lại góp phần vào sự sụp đổ của Hitler. Scherbius đã không sống đủ lâu để chứng kiến sự thành công và thất bại của hệ thống mật mã của ông. Năm 1929, trong khi lái xe ngựa, ông đã bị mất điều khiển, đâm vào tường, và đã qua đời ngày 13 tháng Năm do bị nội thương.

4

Công phá Enigma

Trong những năm tiếp sau Thế chiến Thứ nhất, các nhà giải mã Anh của Phòng 40 vẫn tiếp tục kiểm soát hệ thống thông tin liên lạc của Đức. Vào năm 1926, họ bắt đầu chặn bắt được những bức thư mà họ hoàn toàn không thể giải mã nổi. Vậy là Enigma đã xuất hiện và khi số lượng máy Enigma ngày càng tăng, thì khả năng thu thập thông tin tình báo của Phòng 40 càng giảm đi nhanh chóng. Người Mỹ và Pháp cũng thử phá mật mã Enigma, song những cố gắng của họ cũng thảm bại không kém, và họ nhanh chóng từ bỏ việc hóa giải nó. Người Đức giờ đây đã có một hệ thống thông tin liên lạc an toàn nhất trên thế giới.

Tốc độ từ bỏ hy vọng hóa giải Enigma của các nhà giải mã Đồng minh rõ ràng là ngược hẳn lại với sự kiên nhẫn của họ ngay thập kỷ trước của Thế chiến Thứ nhất. Đứng trước nguy cơ thất bại, các nhà giải mã Đồng minh đã làm việc ngày đêm để xâm nhập mật mã của Đức. Có vẻ như nỗi sợ hãi đã là động lực chính và hiểm họa là một trong những cơ sở cho việc giải mã

thành công. Tương tự, cũng chính là nỗi sợ hãi và hiểm họa đã kích thích các nhà tạo mã Pháp vào cuối thế kỷ 19, khi phải đối mặt với mối đe dọa ngày càng tăng của người Đức. Tuy nhiên, sau Thế chiến Thứ nhất, quân Đồng minh không còn sợ ai nữa. Người Đức đã bị tê liệt bởi thất bại và quân Đồng minh đang ở vị thế trội hơn, và do vậy họ dường như đánh mất hết nhiệt huyết của mình đối với mật mã. Các nhà giải mã của quân Đồng minh đã thu hẹp dần về số lượng và giảm dần về chất lượng.

Tuy nhiên, có một quốc gia không chịu nghỉ ngơi. Sau Thế chiến Thứ nhất, Ba Lan đã tự thiết lập lại một nhà nước độc lập, song quốc gia này vẫn còn lo ngại sự đe dọa từ những đế quốc mới xuất hiện. Phía đông là nước Nga, một quốc gia có tham vọng mở rộng chủ nghĩa cộng sản và phía tây là nước Đức, đang khát khao muốn lấy lại phần lãnh thổ đã phải nhường lại cho Ba Lan sau chiến tranh. Bị kẹp giữa hai đối thủ này, Ba Lan rất khát thông tin tình báo và họ đã lập ra một văn phòng mật mã mới, có tên là Biuro Szyfrów. Nếu sự cần thiết là mẹ đẻ của phát minh thì có lẽ hiểm họa chính là mẹ đẻ của khoa giải mã. Sự thành công của Biuro Szyfrów được minh họa bởi thắng lợi của họ trong suốt cuộc chiến tranh Nga - Ba Lan trong những năm 1919-20. Chỉ trong tháng Tám năm 1920, khi quân đội Xôviết ở cửa ngõ Vácsava, Biuro đã giải mã được 400 bức thư của đối phương. Sự kiểm soát thông tin liên lạc Đức của họ cũng có hiệu quả tương tự cho đến năm 1926, khi họ cũng chạm trán với những bức thư mã hóa bằng máy Enigma.

Nhiệm vụ giải mã các bức thư của Đức thuộc về Đại úy Maksymilian Ciezki, một người yêu nước nhiệt thành, lớn lên ở thị trấn Szamotuty, trung tâm của chủ nghĩa dân tộc Ba Lan.

Ciezki đã được tiếp cận với một máy Enigma thương mại và biết được tất cả các nguyên lý trong phát minh của Scherbius. Nhưng không may là loại máy thương mại này hoàn toàn khác biệt với máy dùng cho quân đội ở cách nối dây bên trong các đĩa mã hóa. Vì không biết gì về cách nối dây bên trong máy mã hóa dùng trong quân đội, nên Ciezki đã không thể giải mã các bức thư được gửi đi từ quân đội Đức. Ông nản lòng đến mức thậm chí đã thuê một nhà ngoại cảm có khả năng thấu thị thử thâu tóm ý nghĩa nào đó từ những bức thư mã hóa bắt được. Tất nhiên, là người này đã thất bại khi không thu được kết quả như Biuro Szyfrów mong muốn. Thay vào đó, công lao lại thuộc về một người Đức bất mãn, Hans-Thilo Schmidt, người đã đi bước đầu tiên trong quá trình công phá mật mã Enigma.

Hans-Thilo Schmidt sinh năm 1888 tại Berlin, là con trai thứ hai của một giáo sư nổi tiếng và người vợ có dòng dõi quý tộc. Schmidt khởi nghiệp trong Quân đội Đức và đã tham gia chiến đấu trong Thế chiến Thứ nhất, song ông đã không được đánh giá một cách xứng đáng và đã bị phục viên trong chương trình cắt giảm quân số mạnh mẽ được thực hiện như là một phần của Hiệp ước Versailles. Sau đó ông đã thử kinh doanh nhưng nhà máy xà phòng của ông đã bị buộc phải đóng cửa vì khủng hoảng và siêu lạm phát thời kỳ hậu chiến, khiến ông và cả gia đình trở nên túng quẫn.

Sự tủi hổ trước thất bại của Schimidt lại càng tăng thêm bởi sự thành đạt của anh trai ông, Rudolph, người cũng đã chiến đấu trong chiến tranh, nhưng sau đó vẫn tiếp tục được tại ngũ. Trong suốt những năm 1920, Rudolph liên tục được thăng chức và cuối cùng đã được đề bạt làm Tham mưu trưởng binh chủng

Hans-Thilo Schmidt

Thông tin. Ông là người chịu trách nhiệm đảm bảo thông tin liên lạc an toàn và trong thực tế Rudolph cũng chính là người cấp phép sử dụng mật mã Enigma.

Sau khi việc kinh doanh lụn bại, Hans-Thilo đã buộc phải nhờ người anh giúp đỡ và Rudolph đã sắp xếp một công việc cho ông ở Chiffrierstelle, một văn phòng chịu trách nhiệm quản lý thông tin liên lạc mã hóa, ở Berlin. Đây là trung tâm chỉ huy của Enigma, một tổ chức tối mật và chỉ xử lý những thông tin có độ nhạy cảm cao. Khi Hans-Thilo chuyển công việc mới, ông để gia đình ở lại Bavaria, nơi có giá cả sinh hoạt dễ chịu hơn. Ông sống một mình ở thành phố Berlin đắt đỏ, kiệt quệ và đơn độc, ghen tỵ với người anh thành đạt của mình và bực tức với đất nước đã chối bỏ ông. Kết quả là không thể tránh khỏi. Bằng cách bán các thông tin mật về Enigma cho các thế lực nước ngoài, Hans-Thilo Schmidt đã kiếm được tiền và trả được mối thù hận, phá hoại an ninh của đất nước và làm hại thanh danh tổ chức của chính anh trai mình.

Ngày 8 tháng Mười một năm 1931, Schmidt đến khách sạn Grand ở Verviers, Bỉ để liên lạc với một điệp viên mật của Pháp với bí danh là Rex. Với cái giá 10.000 mác (tương đương với 30.000 đôla ngày nay), Schmidt đã để cho Rex sao chụp hai tài

liệu: *Gebrauchsanweisung für die Chiffriermaschine Enigma* và *Schlüsselanleitung für die Chiffriermaschine Enigma*. Các tài liệu này hướng dẫn cách sử dụng máy Enigma và mặc dù không có sự mô tả chi tiết cách nối dây bên trong mỗi đĩa mã hóa song chúng cũng chứa những thông tin cần thiết để suy luận ra cách nối dây đó.

Nhờ có sự phản bội của Schmidt, giờ đây quân Đồng minh đã có thể tạo ra một bản sao chính xác của máy Enigma dùng trong quân đội Đức. Tuy nhiên, điều này cũng vẫn chưa đủ để họ có thể giải được các bức thư mã hóa bằng Enigma. Sức mạnh của mật mã không phụ thuộc vào việc giữ bí mật về máy mà là giữ bí mật về sự cài đặt ban đầu (khóa mã) của máy. Nếu nhà giải mã muốn giải mã một bức thư chặn bắt được thì ngoài việc có một bản sao máy Enigma, anh ta vẫn phải tìm trong số hàng triệu tỉ khóa mã tiềm năng một khóa mã đã được sử dụng để mã hóa nó. Một bản ghi nhớ của người Đức có viết như thế này: "Trong việc đánh giá độ an toàn của hệ thống mã hóa phải giả định là kẻ thù đã có trong tay chiếc máy đó."

Cơ quan Mật vụ của Pháp rõ ràng đã sẵn sàng vào cuộc, khi họ tìm được người đưa tin cho Schmidt và có được tài liệu nói về cách nối dây bên trong máy Enigma dùng trong quân đội. Trong khi đó, các nhà giải mã Pháp lại không mấy mặn mà, và dường như chưa sẵn sàng và do đó không thể khai thác các thông tin mới thu được này. Trong bối cảnh Thế chiến Thứ nhất kết thúc, họ đã tỏ ra quá tự tin và thiếu năng động. Văn phòng Mật mã thậm chí không buồn cố gắng chế tạo một bản sao máy Enigma dùng trong quân đội, vì họ cho rằng việc đạt được bước tiếp theo, tức là tìm ra khóa mã cần dùng để mã hóa cho một bức thư cụ thể nào đó trên máy Enigma, là không thể thực hiện được.

Khi điều này xảy ra thì Pháp đã ký một hiệp định về hợp tác quân sự với Ba Lan được mười năm. Ba Lan đã biểu lộ sự quan tâm đến bất kỳ thứ gì liên quan đến Enigma, vì vậy, căn cứ vào hiệp định có từ mười năm trước, người Pháp đã đơn giản chuyển tài liệu sao chụp được của Schmidt cho Đồng minh của mình và chuyển nhiệm vụ vô vọng là hóa giải Enigma cho Biuro Szyfrów. Biuro nhận thấy rằng các tài liệu này mới chỉ là điểm khởi đầu, song không giống người Pháp, họ bị nỗi sợ bị xâm lược thúc đẩy. Người Ba Lan tự thuyết phục mình rằng phải có một con đường tắt để tìm ra khóa mã của một bức thư mã hóa bằng Enigma, và nếu họ tập trung được đầy đủ nỗ lực, sự sáng tạo và trí tuệ thì họ có thể tìm ra con đường ngắn nhất đó.

Cùng với việc tiết lộ các thông tin về cách nối dây bên trong các đĩa mã hóa, các tài liệu của Schmidt còn giải thích chi tiết cách bố trí của sổ mã được người Đức sử dụng. Mỗi tháng, những người điều khiển Enigma lại nhận được một sổ mã mới trong đó ghi rõ khóa mã sử dụng hằng ngày. Chẳng hạn, trong ngày đầu tiên của tháng, sổ mã có thể cung cấp *khóa mã ngày* như sau:

(1) *Cài đặt của bảng ổ nối*: A/L - P/R - T/D - B/W - K/F - O/Y
(2) *Sắp xếp của các đĩa mã hóa*: 2-3-1
(3) *Định hướng của các đĩa mã hóa*: Q-C-W

Sắp xếp và định hướng của đĩa mã hóa được gọi là cài đặt đĩa mã hóa. Để thực hiện khóa mã cụ thể này, người điều khiển máy Enigma sẽ cài đặt máy của mình như sau:

(1) *Cài đặt bảng ổ nối*: hoán đổi chữ cái A và L bằng cách nối chúng với nhau bằng một dây dẫn trên bảng, tương tự như thế với P và R, T và D, B và W, K và F và cuối cùng là O và Y.

(2) *Sắp xếp đĩa mã hóa*: Đặt đĩa mã hóa thứ hai ở khe thứ nhất của máy, đĩa mã hóa thứ ba ở khe thứ hai và đĩa thứ nhất ở khe thứ ba.

(3) *Định hướng đĩa mã hóa*: Mỗi đĩa mã hóa đều có bảng chữ cái khắc trên vành ngoài của nó, điều này cho phép người điều khiển đặt nó ở một định hướng nhất định. Trong trường hợp này, người điều khiển sẽ quay đĩa ở khe số một sao cho chữ cái Q hướng lên trên, quay đĩa ở khe số hai để sao cho chữ cái C hướng lên trên và quay đĩa ở khe số ba sao cho chữ cái W hướng lên trên.

Một cách mã hóa thông tin đó là người gửi mã hóa tất cả thư từ một ngày theo khóa mã ngày. Điều này có nghĩa là trong cả một ngày, từ bức thư đầu tiên, tất cả những người điều khiển Enigma đều phải cài đặt máy của họ theo cùng một khóa mã ngày. Sau đó, mỗi khi một bức thư cần phải gửi đi, trước tiên nó sẽ được đánh vào máy; bản mã hóa sẽ được ghi lại và chuyển cho điện báo viên vô tuyến để truyền đi. Ở đầu kia, người nhận sẽ ghi lại thư đến, chuyển nó cho người điều khiển Enigma, người này cũng đánh vào máy đã được cài đặt theo cùng khóa mã ngày. Kết quả là sẽ nhận được bức thư gốc.

Quá trình này tương đối an toàn song nó lại có điểm yếu là sử dụng mỗi một khóa mã cho hàng trăm bức thư gửi đi trong ngày. Nói chung, sẽ rất đúng nếu nói rằng việc chỉ sử dụng một khóa mã để mã hóa một khối lượng thông tin khổng lồ sẽ tạo điều kiện cho người giải mã dễ suy luận hơn. Một lượng lớn thông tin được mã hóa như nhau sẽ cho nhà giải mã cơ hội còn lớn hơn nữa đối với việc xác định khóa mã. Chẳng hạn, quay trở lại những mật

mã đơn giản hơn, giải một mật mã dùng một bảng chữ cái bằng phương pháp phân tích tần suất sẽ đơn giản hơn nhiều nếu có một vài trang thông tin được mã hóa so với khi chỉ có một vài câu.

Vì vậy, để cẩn trọng hơn, người Đức đã đi một bước thông minh hơn trong việc sử dụng khóa mã ngày để chuyển *khóa mã thư* mới cho mỗi bức thư. Khóa mã thư cũng có cùng cách cài đặt bảng ổ nối và sắp xếp đĩa mã hóa như khóa mã ngày, nhưng sự định hướng của các đĩa mã hóa thì khác. Vì sự định hướng mới của các đĩa mã hóa không có trong sổ mã nên người gửi phải chuyển nó một cách an toàn cho người nhận theo qui trình như sau. Đầu tiên, người gửi cài đặt máy của mình theo khóa mã ngày đã thống nhất, kể cả định hướng của các đĩa mã hóa, ở ví dụ trên là **QCW**. Sau đó, anh ta sẽ lựa chọn ngẫu nhiên một định hướng mới cho các đĩa mã hóa để làm khóa mã thư, chẳng hạn **PGH**. Sau đó, mã hóa **PGH** theo khóa mã ngày. Khóa mã thư được đánh vào máy Enigma hai lần, cốt là để người nhận kiểm tra lại. Chẳng hạn, người gửi có thể mã hóa khóa mã thư là **PGHPGH** thành **KIVBJE**. Hãy lưu ý là hai nhóm chữ cái **PGH** được mã hóa khác nhau (đầu tiên là **KIV** và sau là **BJE**) vì các đĩa mã hóa Enigma quay sau mỗi một chữ cái và thay đổi toàn bộ cách mã hóa. Người gửi sau đó thay đổi máy của mình theo định hướng **PGH** và mã hóa bức thư chính theo khóa mã thư này. Ở chỗ người nhận, cài đặt ban đầu của máy theo khóa mã ngày, tức là **QCW**. Sáu chữ cái đầu tiên của bức thư đến, đó là **KIVBJE**, được đánh vào và cho **PGHPGH**. Người nhận sau đó sẽ cài đặt máy của mình theo định hướng **PGH**, khóa mã thư, và sau đó có thể giải mã phần chính của bức thư.

Điều này đồng nghĩa với việc người gửi và người nhận thống nhất với nhau một khóa mã chính. Sau đó, thay vì sử dụng khóa

mã chính này để mã hóa tất cả các bức thư thì họ chỉ sử dụng để mã hóa một khóa mã mới cho mỗi bức thư và mã hóa phần nội dung chính theo khóa mã mới. Nếu người Đức không sử dụng khóa mã thư thì tất cả - có lẽ là phải đến hàng ngàn thông tin với hàng triệu chữ cái - được gửi đi với cùng khóa mã ngày. Tuy nhiên, nếu khóa mã ngày chỉ được sử dụng để truyền khóa mã thư thì nó chỉ mã hóa một lượng nhỏ chữ cái. Nếu có 1.000 khóa mã thư được gửi đi trong một ngày thì khóa mã ngày chỉ mã hóa 6.000 chữ cái. Và vì mỗi khóa mã thư được lựa chọn ra một cách ngẫu nhiên và chỉ được sử dụng để mã hóa một bức thư thì nó mã hóa một lượng rất ít chữ cái, có lẽ chỉ vào khoảng vài trăm ký tự.

Thoạt trông thì hệ thống này dường như không thể hóa giải, song các nhà giải mã Ba Lan đã không chịu khuất phục. Họ đã được chuẩn bị để khám phá tất cả các con đường nhằm tìm ra điểm yếu của máy Enigma và cách sử dụng khóa mã ngày và khóa mã thư của nó. Điều quan trọng nhất trong cuộc chiến chống lại Enigma, đó là một thế hệ các nhà giải mã mới. Trong nhiều thế kỷ, gần như mặc định rằng các nhà giải mã giỏi nhất phải là các chuyên gia về cấu trúc ngôn ngữ, song sự xuất hiện của Enigma đã khiến người Ba Lan phải thay đổi chính sách tuyển dụng của mình. Enigma là một dạng mật mã máy và Biuro Szyfrów hiểu rằng phải những bộ não khoa học hơn mới có được cơ hội tốt hơn trong việc hóa giải nó. Biuro đã tổ chức một khóa đào tạo về mật mã và mời hai mươi nhà toán học, mỗi người đều phải tuyên thệ giữ bí mật. Tất cả các nhà toán học này đều tới từ trường đại học Poznán. Mặc dù đây không phải là một trung tâm khoa học danh tiếng ở Ba Lan, song nó có lợi thế là được đặt ở miền tây,

trong vùng lãnh thổ mà trước năm 1918 là thuộc Đức. Vì vậy các nhà toán học này đều thông thạo tiếng Đức.

Ba trong số hai mươi người này đã chứng minh được khả năng xử lý mật mã và được tuyển dụng vào Biuro. Tài năng nhất trong số họ là Marian Rejewski, một thanh niên cận thị, 23 tuổi, tính tình nhút nhát, trước đây đã từng học ngành thống kê vì muốn theo nghề bảo hiểm. Mặc dù là một sinh viên ưu tú trong trường đại học song chỉ đến khi vào Biuro Szyfrów, Marian mới nhận ra thiên hướng thực sự của mình. Anh đã hóa giải được một loạt các mật mã truyền thống trong thời gian tập sự trước khi tiến tới một thử thách khó khăn hơn, là Enigma. Làm việc hoàn toàn độc lập, anh tập trung tất cả sức lực vào sự phức tạp của cỗ máy của Scherbius. Là một nhà toán học, anh sẽ phải cố gắng phân tích mọi khía cạnh trong sự vận hành của máy, xem xét tác dụng của các đĩa mã hóa và của các cách nối dây trong bảng ổ nối. Tuy nhiên, cũng giống như với toàn bộ toán học, công việc của anh đòi hỏi cả sự cảm hứng lẫn logic. Như một nhà giải mã toán học khác trong thời chiến đã nói, nhà giải mã sáng tạo là phải "chung đụng hằng ngày với những bóng ma đen tối để đạt được những chiến công của môn võ thuật tinh thần này".

Chiến lược tấn công Enigma của Rejewski dựa trên thực tế là, sự lặp lại chính là kẻ thù của an toàn: sự lặp lại dẫn đến các khuôn mẫu và nhà giải mã sẽ khai thác từ các khuôn mẫu đó. Sự lặp lại rõ ràng nhất trong mã hóa bằng Enigma đó chính là khóa mã thư, được mã hóa hai lần ở đầu mỗi bức thư. Nếu người điều khiển máy chọn khóa mã thư là **ULJ**, thì anh ta sẽ mã hóa nó hai lần, tức là **ULJULJ** có thể được mã hóa thành **PEFNWZ**, mà sau đó anh ta sẽ gửi ngay trước nội dung thực sự của bức thư.

Người Đức cần sự lặp lại này để tránh nhầm lẫn do nhiễu sóng vô tuyến hoặc do lỗi của người điều khiển. Song họ không dự liệu trước được rằng chính điều này có thể gây phương hại đến sự an toàn của máy.

Mỗi ngày, Rejewski lại tự mình nghiên cứu những chuyến thư mới bắt được. Tất cả số thư từ đó đều bắt đầu bằng sáu chữ cái của khóa mã thư gồm ba chữ cái lặp lại, đều được mã hóa theo cùng khóa mã ngày đã được thỏa thuận từ trước. Chẳng hạn, anh nhận được bốn bức thư bắt đầu bằng các khóa mã thư được mã hóa như sau:

Chữ cái thứ	1	2	3	4	5	6
Thư thứ nhất	L	O	K	R	G	M
Thư thứ hai	M	V	T	X	Z	E
Thư thứ ba	J	K	T	M	P	E
Thư thứ tư	D	V	T	P	Z	X

Trong mỗi trường hợp, các chữ cái thứ nhất và thứ tư là mã hóa của cùng một chữ cái, đó là chữ cái đầu tiên của khóa mã thư. Chữ cái thứ hai và thứ năm cũng là mã hóa của cùng một chữ cái, là chữ cái thứ hai của khóa mã thư, và chữ cái thứ ba và thứ sáu là mã hóa của cùng một chữ cái, là chữ cái thứ ba của khóa mã thư. Chẳng hạn, trong bức thư thứ nhất, chữ L và R là mã hóa của cùng một chữ cái, chữ cái đầu tiên của khóa mã thư. Lý do tại sao cùng một chữ cái này lại được mã hóa khác nhau, đầu tiên là L và sau đó là R, đó là vì giữa hai lần mã hóa, đĩa mã hóa thứ nhất của máy Enigma đã quay đi ba nấc, làm thay đổi toàn bộ cách mã hóa.

Thực tế L và R là mã hóa của cùng một chữ cái đã giúp cho Rejewski suy luận ra một sự ràng buộc nhỏ nào đó về sự cài đặt

ban đầu của máy. Sự cài đặt ban đầu của các đĩa mã hóa, vẫn chưa biết, đã mã hóa chữ cái đầu tiên của khóa mã thư, cũng chưa biết, thành **L**, và sau đó một sự cài đặt khác của các đĩa mã hóa, cách sự cài đặt ban đầu ba bước mà ta vẫn còn chưa biết, đã mã hóa cùng chữ cái đó của khóa mã thư thành **R**.

Ràng buộc này dường như khá mờ nhạt vì quá nhiều ẩn số, song ít nhất thì nó cũng cho biết **L** và **R** có quan hệ mật thiết với nhau bởi cách cài đặt ban đầu của máy Enigma, đó là khóa mã ngày. Từ mỗi bức thư mới chặn bắt được, người ta lại xác định được các mối quan hệ khác giữa chữ cái thứ nhất và thứ tư của khóa mã thư. Tất cả các mối quan hệ này đều phản ánh cách cài đặt ban đầu của máy Enigma. Chẳng hạn, bức thư thứ hai ở trên cho chúng ta biết **M** và **X** có liên quan với nhau, bức thư thứ ba cho biết **J** và **M** có quan hệ, và bức thư thứ tư cho biết **D** và **P** có quan hệ. Rejewski tóm tắt lại các mối quan hệ này bằng cách lập bảng. Với bốn lá thư chúng ta có lúc này, bảng sẽ phản ánh các mối quan hệ giữa **(L,R)**, **(M,X)**, **(J,M)** và **(D,P)**:

Chữ cái thứ nhất	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chữ cái thứ tư																P						M		R	X	

Nếu Rejewski có đủ số thư của cả một ngày thì anh sẽ có thể hoàn tất bảng chữ cái các mối quan hệ. Bảng dưới đây là một bảng quan hệ hoàn chỉnh như vậy:

Chữ cái thứ nhất	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chữ cái thứ tư	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

Marian Rejewski

Rejewski không biết khóa mã ngày và anh cũng không biết khóa mã thư nào được lựa chọn nhưng anh biết rằng chúng được tạo nên trong bảng quan hệ này. Nếu khóa mã ngày là khác thì bảng các mối quan hệ cũng sẽ hoàn toàn khác. Câu hỏi tiếp theo được đặt ra là liệu có cách nào cho phép xác định được khóa mã ngày từ bảng các mối quan hệ hay không. Rejewski bắt tay tìm kiếm các khuôn mẫu trong bảng, tức là các cấu trúc có thể chỉ ra khóa mã ngày. Cuối cùng, anh đã bắt tay nghiên cứu một loại khuôn mẫu đặc biệt, tạo nên một vòng các chữ cái. Ví dụ, trong bảng, chữ cái **A** ở hàng trên gắn với **F** ở hàng dưới, tiếp đó, anh lại tìm **F** ở hàng trên, thì thấy nó gắn với **W** ở hàng dưới và rồi anh tiếp tục tìm **W** ở hàng trên thì thấy **W** lại gắn với **A**, là điểm mà chúng ta bắt đầu. Tức là khép kín một vòng.

Với các chữ cái còn lại trong bảng, Rejewski tìm được thêm các vòng khác. Anh liệt kê tất cả các vòng và ghi chú số các liên kết trong đó:

A →F →W →A	3 liên kết
B →Q →Z →K →V →E →L →R →I →B	9 liên kết
C →H →G →O →Y →D →P →C	7 liên kết
J →M →X →S →T →N →U →J	7 liên kết

Cho tới đây, chúng ta mới chỉ xem xét liên kết giữa chữ cái thứ nhất và thứ tư của khóa mã lặp lại gồm sáu chữ cái. Còn trong thực tế, Rejewski phải thực hiện công việc này đối với cả mối liên hệ giữa các chữ cái thứ hai và thứ năm, thứ ba và thứ sáu, tức là xác định các vòng liên kết ở mỗi trường hợp và xác định số liên kết ở mỗi vòng.

Rejewski nhận thấy rằng các vòng liên kết thay đổi hằng ngày. Đôi khi có rất nhiều vòng ngắn, đôi khi lại có một số vòng dài. Và tất nhiên, các chữ cái trong các vòng cũng thay đổi. Đặc điểm của các vòng rõ ràng là kết quả của việc cài đặt khóa mã ngày - một hệ quả tổng hợp của việc cài đặt bảng ổ nối, sự sắp đặt các đĩa mã hóa và định hướng các đĩa mã hóa. Tuy nhiên, có một câu hỏi nữa, đó là làm thế nào Rejewski có thể xác định được *khóa mã ngày* từ các vòng liên kết này. Khóa mã nào trong số 10.000.000.000.000.000 khóa mã tiềm năng có liên quan đến một khuôn mẫu nhất định của các vòng liên kết? Số các khả năng đơn giản là quá lớn.

Chính đây là lúc mà Rejewski có được sự thấu hiểu sâu sắc. Mặc dù sự cài đặt của bảng ổ nối và các đĩa mã hóa đều ảnh hưởng đến những chi tiết của các vòng liên kết, song sự đóng góp của chúng ở một mức độ nào đó là có thể tháo gỡ được. Đặc biệt, có một tính chất của các vòng liên kết chỉ phụ thuộc hoàn toàn vào sự cài đặt của các đĩa mã hóa chứ không liên quan gì đến bảng ổ nối, đó là: số lượng các liên kết chỉ là kết quả của sự cài đặt các đĩa mã hóa. Chẳng hạn, chúng ta hãy xem xét lại ví dụ trên và giả sử rằng khóa mã ngày đòi hỏi chữ cái **S** và **G** hoán đổi cho nhau trên bảng ổ nối. Nếu chúng ta thay đổi yếu tố này của khóa mã ngày, bằng cách tháo bỏ dây cáp

nối giữa **S** và **G**, và thay vào đó là **T** và **K**, thì các vòng liên kết sẽ thay đổi như sau:

A →F →W →A	3 liên kết
B →Q →Z →T →V →E →L →R →I →B	9 liên kết
C →H →S →O →Y →D →P →C	7 liên kết
J →M →X →G →K →N →U →J	7 liên kết

Một số chữ cái trong các vòng liên kết đã thay đổi, nhưng, điều quan trọng là số các liên kết của mỗi vòng vẫn giữ nguyên. Vậy là Rejewski đã tìm ra một đặc điểm của các vòng liên kết chỉ phản ánh sự cài đặt của các đĩa mã hóa.

Tổng số cách cài đặt các đĩa mã hóa bằng số cách sắp xếp các đĩa này (6) nhân với số định hướng của các đĩa đó (17.576), tức là 105.456. Như vậy, thay vì phải lo âu với con số 10.000.000.000.000.000 khóa mã ngày gắn với một tập hợp các vòng liên kết nhất định thì giờ đây Rejewski chỉ phải bận tâm đến một vấn đề đơn giản hơn rất nhiều: đó là cách nào trong số 105.456 cách cài đặt các đĩa mã hóa gắn với số các liên kết trong một tập hợp các vòng? Con số này tuy vẫn còn rất lớn song nó đã nhỏ hơn hàng trăm tỉ lần so với tổng số các khóa mã ngày tiềm năng. Nói gọn lại, nhiệm vụ trở nên đơn giản hơn hàng trăm tỉ lần, chắc chắn là trong tầm cố gắng của con người.

Rejewski tiếp tục tiến hành như sau. Nhờ có sự phản bội của Hans-Thilo Schmidt, anh đã tiếp cận được với các bản sao máy Enigma. Nhóm của anh bắt đầu một công việc cực kỳ vất vả là thử tất cả 105.456 cách cài đặt các đĩa mã hóa, và lập bảng tổng hợp độ dài của các vòng liên kết do mỗi cách cài đặt đó tạo ra. Họ phải mất ròng rã một năm trời để hoàn thành bảng tổng hợp

đó, và một khi Biuro tích lũy được đủ dữ liệu thì Rejewski cuối cùng cũng đã có thể bắt đầu công phá mật mã Enigma.

Mỗi ngày, anh lại nghiên cứu các khóa mã thư đã được mã hóa, chính là sáu chữ cái đầu tiên trong tất cả các bức thư chặn bắt được, và sử dụng thông tin đó để lập bảng các mối quan hệ. Điều này cho phép anh tìm ra các vòng liên kết, và số các liên kết trong mỗi vòng. Ví dụ, khi phân tích các chữ cái thứ nhất và thứ tư có thể tìm ra bốn vòng liên kết với số liên kết là 3, 9, 7 và 7. Phân tích chữ cái thứ hai và năm cũng cho bốn vòng với số liên kết là 2, 3, 9 và 12. Phân tích chữ cái thứ ba và sáu cho năm vòng liên kết với số liên kết là 5, 5, 5, 3 và 8. Như vậy, mặc dù Rejewski không biết khóa mã ngày song anh biết rằng nó tạo ra ba tập hợp các vòng liên kết với số vòng và số liên kết trong mỗi vòng như sau:

4 vòng từ chữ cái thứ 1 và thứ 4, với 3, 9, 7 và	7 liên kết
4 vòng từ chữ cái thứ 2 và thứ 5, với 2, 3, 9 và	12 liên kết
5 vòng từ chữ cái thứ 3 và thứ 6, với 5, 5, 5, 3 và	8 liên kết

Giờ thì Rejewski có thể đối chiếu với bảng tổng hợp của mình, trong đó có chứa mọi cách sắp đặt các đĩa mã hóa được lập theo loại vòng mà nó tạo ra. Nhờ có các số liệu trong bảng tổng hợp, gồm số vòng và số các liên kết trong ở mỗi vòng, anh ngay lập tức biết được cách sắp đặt các đĩa mã hóa của khóa mã ngày. Như vậy, các vòng cũng tựa như dấu vân tay, một bằng chứng cho biết sự định hướng và sự sắp đặt của các đĩa mã hóa. Rejewski làm việc như một viên thám tử tìm dấu vân tay ở hiện trường vụ án và sau đó sử dụng cơ sở dữ liệu để truy tìm kẻ nghi vấn.

Mặc dù đã xác định được phần đĩa mã hóa trong khóa mã

ngày, song Rejewski còn phải tìm ra cách cài đặt ở bảng ổ nối. Tuy có tới hàng trăm tỉ khả năng song nó là một nhiệm vụ tương đối đơn giản. Rejewski bắt đầu bằng việc sắp đặt các đĩa mã hóa trong bản sao máy Enigma theo phần đĩa mã hóa mới được xác lập của khóa mã ngày. Sau đó anh rút tất cả các dây cáp ra khỏi bảng ổ nối, và như vậy bảng ổ nối sẽ không còn ảnh hưởng gì nữa. Cuối cùng, anh lấy một đoạn văn bản mật mã chặn bắt được và đánh vào máy Enigma. Phần lớn sẽ tạo ra các từ vô nghĩa, vì cách nối dây trong bảng ổ nối vẫn còn chưa biết và đã bị rút ra. Tuy nhiên, cũng thường xuất hiện những cụm từ có thể lờ mờ nhận ra, chẳng hạn như **alliveinbelrin** - có thể phỏng đoán rằng nó có thể là "arrive in Berlin" (đến Berlin). Nếu giả định này là đúng thì nó cho biết chữ cái **R** và **L** có thể đã được nối và hoán đổi cho nhau bằng dây cáp trong bảng ổ nối, trong khi các chữ cái **A**, **I**, **V**, **E**, **B** và **N** thì không. Bằng cách phân tích các cụm từ khác, có thể xác định được năm cặp chữ cái còn lại đã được hoán đổi bởi bảng ổ nối. Sau khi đã thiết lập được cách cài đặt bảng ổ nối và khám phá ra sự sắp đặt các đĩa mã hóa, Rejewski đã tìm ra khóa mã ngày và sau đó có thể giải mã được bất kỳ bức thư bí mật nào được gửi đi trong ngày.

Rejewski đã làm cho nhiệm vụ tìm khóa mã ngày đơn giản đi rất nhiều bằng cách tách riêng việc tìm cách sắp đặt các đĩa mã hóa và việc tìm cách cài đặt bảng ổ nối. Và xét một cách riêng rẽ, thì cả hai vấn đề trên đều có thể giải quyết được. Ban đầu, chúng ta ước tính rằng sẽ phải mất một khoảng thời gian nhiều hơn cả tuổi của vũ trụ để thử tất cả các khóa mã khả dĩ của Enigma. Tuy nhiên, Rejewski chỉ mất một năm để soạn bảng tổng hợp độ dài của các vòng, và sau đó thì anh có thể tìm ra khóa mã ngày

trước khi một ngày trôi qua. Một khi đã có khóa mã ngày thì anh cũng có đủ thông tin như người nhận đã định và do vậy có thể giải mã một cách dễ dàng.

Sau khi có phát minh của Rejewski, hệ thống thông tin liên lạc của người Đức trở nên "trong suốt". Người Ba Lan chưa phải lâm vào chiến tranh với người Đức, song mối đe dọa bị xâm lược thì vẫn treo lơ lửng đó và do vậy mà niềm vui của người Ba Lan trước việc chinh phục được Enigma là vô cùng to lớn. Nếu họ biết được các tướng lĩnh Đức đang toan tính những gì thì họ sẽ có cơ hội để tự phòng vệ. Vận mệnh của đất nước Ba Lan phụ thuộc vào Rejewski và anh đã không làm cho tổ quốc mình phải thất vọng. Sự tấn công của Rejewski vào Enigma thực sự là một trong những chiến công giải mã vĩ đại nhất. Tôi đã tóm tắt công việc của anh chỉ trong vài trang giấy và đã lược bỏ bớt những chi tiết kỹ thuật cũng như những bế tắc mà anh đã gặp phải. Enigma là một máy mã hóa phức tạp và việc hóa giải nó đòi hỏi phải huy động một trí lực khổng lồ. Sự đơn giản hóa của tôi chắc đã không khiến các bạn đánh giá thấp đi thành tựu phi thường của Rejewski.

Thành công của người Ba Lan trong việc hóa giải mật mã Enigma là nhờ có ba yếu tố: nỗi sợ hãi, toán học và gián điệp. Nếu không có nỗi lo sợ bị xâm lược thì người Ba Lan đã bị nhụt chí trước mật mã Enigma rõ ràng là không thể hóa giải. Không có toán học thì Rejewski cũng sẽ không thể phân tích được các vòng. Và nếu không có Schmidt, với mật danh "Asche", và các tài liệu do ông ta cung cấp thì các cách nối dây trong các đĩa mã hóa sẽ không được biết đến và việc phân tích mã thậm chí không thể được bắt đầu. Rejewski đã không hề do dự nhấn mạnh đến món

nợ mà ông mang ơn Schmidt: "Các tài liệu của Asche được đón đợi như bánh manna rơi xuống từ thiên đường và tất cả các cánh cửa đã được mở ra tức thì".

Người Ba Lan đã sử dụng thành công kỹ thuật của Rejewski trong vài năm. Khi Hermann Gôring đến thăm Vácsava vào năm 1934, ông ta đã hoàn toàn không ý thức được rằng hệ thống liên lạc của mình bị chặn bắt và giải mã. Khi ông ta và các quan chức khác của Đức đến đặt vòng hoa trước Mộ các Chiến sĩ Vô danh bên cạnh văn phòng của Biuro Szyfrów, Rejewski có thể đã đứng nhìn họ từ trên cửa sổ, hài lòng về những thông tin mà ông đọc được từ hệ thống liên lạc tối mật của Đức.

Ngay cả khi người Đức có một thay đổi nhỏ trong cách truyền thông tin thì Rejewski cũng đánh bại họ. Bảng tổng hợp độ dài các vòng trước đây của ông không còn sử dụng được nữa, nhưng thay vì viết lại bảng tổng hợp khác, ông đã phát minh ra một hệ thống tổng hợp bằng máy, nó có thể tự động tìm kiếm cách sắp đặt đúng của các đĩa mã hóa. Phát minh của Rejewski là một sự điều chỉnh thích hợp với máy Enigma, nó có thể kiểm tra một cách nhanh chóng tất cả 15.576 cách sắp đặt cho đến khi tìm ra cách thích hợp. Vì có sáu khả năng sắp xếp các đĩa mã hóa nên sẽ cần phải có sáu máy của Rejewski làm việc đồng thời, mỗi máy đại diện cho một cách sắp xếp. Cùng với nhau, chúng tạo thành một bộ máy cao gần 1 mét, có thể tìm kiếm khóa mã ngày chỉ trong khoảng hai giờ. Bộ máy này được gọi là *bom*, một cái tên có thể diễn đạt được những âm thanh ầm ĩ phát ra trong khi các máy này tìm kiếm cách sắp đặt các đĩa mã hóa. Một cách giải thích khác đó là, người ta cho rằng Rejewski đã có ý tưởng về bộ máy này khi đang ở trong một quán cà phê ăn *bom*, một loại

kem có hình bán cầu. *Bom* đã cơ khí hóa một cách hiệu quả quá trình giải mã. Đây là một sự đáp trả tự nhiên đối với Enigma, một sự cơ khí hóa việc mã hóa.

Hầu như trong suốt những năm 1930, Rejewski và đồng nghiệp của anh đã làm việc không mệt mỏi để khám phá ra chìa khóa giải mã Enigma. Hết tháng này đến tháng khác, nhóm đã phải đối mặt với sức ép và sự căng thẳng của việc giải mã, liên tục phải sửa chữa những lỗi kỹ thuật của *bom*, liên tục phải đối mặt với các thư từ bị mã hóa chặn bắt được không ngừng. Cuộc sống của họ bị chi phối bởi việc theo đuổi khóa mã ngày, một phần thông tin sống còn mà nhờ đó có thể khám phá ra ý nghĩa của những bức thư bị mã hóa. Tuy nhiên, những người giải mã Ba Lan không hề biết rằng phần lớn công việc của họ là không cần thiết. Người đứng đầu Biuro là thiếu tá Gwido Langer đã có khóa mã ngày trong tay, nhưng ông giữ kín chúng trong ngăn kéo bàn làm việc của mình.

Langer, qua người Pháp, vẫn nhận được thông tin từ Schmidt. Những hoạt động lén lút của điệp viên người Đức này đã không chấm dứt vào năm 1931 với việc gửi hai tài liệu về cách vận hành của Enigma mà còn tiếp tục trong vòng bảy năm nữa. Ông ta đã gặp điệp viên bí mật người Pháp là Rex hai mươi lần, thường là trong một căn nhà gỗ ở vùng núi biệt lập, nơi mà sự kín đáo được bảo đảm hoàn toàn. Trong mỗi cuộc gặp gỡ đó, Schmidt đã trao một hoặc nhiều cuốn sổ mã, mỗi sổ mã chứa trong đó các khóa mã ngày có giá trị trong một tháng. Đây là những cuốn sổ mã được phân phối cho những người vận hành máy Enigma và có chứa tất cả các thông tin cần thiết để mã hóa và giải mã thông tin. Tính chung lại thì ông ta đã cung cấp các cuốn sổ mã có chứa

khóa mã ngày của 38 tháng. Các khóa mã này lẽ ra đã có thể tiết kiệm được một lượng lớn thời gian và công sức của Rejewski, rút bỏ sự cần thiết của *bom* và dành lại công sức để sử dụng cho những công việc khác của Biuro. Tuy nhiên, Langer khôn ngoan đã quyết định không cho Rejewski biết về các khóa mã này, vì ông đinh ninh rằng làm như thế là chuẩn bị để phòng lúc những khóa mã này không còn có được nữa. Langer biết rằng nếu chiến tranh nổ ra thì Schmidt sẽ không thể tiếp tục tới những cuộc gặp gỡ bí mật và Rejewski sẽ buộc phải độc lập tác chiến. Langer cho rằng Rejewski cần phải rèn luyện tính độc lập trong thời bình, như là một sự chuẩn bị cho những gì đang chờ ở phía trước.

Các kỹ xảo của Rejewski cuối cùng cũng đã đạt tới giới hạn của nó vào tháng Mười hai năm 1938, khi các nhà mã hóa Đức quyết định gia tăng độ an toàn cho Enigma. Những người vận hành Enigma được cung cấp thêm hai đĩa mã hóa mới, như vậy, sự sắp xếp các đĩa mã hóa sẽ là ba đĩa bất kỳ trong số năm đĩa mã hóa sẵn có. Trước đây chỉ có ba đĩa mã hóa (đánh số 1, 2 và 3) để lựa chọn và chỉ có sáu cách sắp xếp chúng, nhưng nay có thêm hai đĩa mã hóa nữa (4 và 5) và số cách sắp xếp bây giờ tăng lên là 60, như trình bày ở Bảng 10. Thách thức đầu tiên với Rejewski đó là phải tìm ra các cách nối dây bên trong hai đĩa mã hóa mới. Đáng lo ngại hơn là, anh phải chế tạo gấp mười lần số máy *bom*, mỗi máy đại diện cho một cách sắp xếp cụ thể của các đĩa mã hóa. Chỉ riêng chi phí để chế tạo một bộ các máy *bom* đã gấp mười lần ngân sách chi cho trang thiết bị hàng năm của Biuro. Sang đến tháng sau, tình trạng lại còn tồi tệ hơn nữa khi số các dây cáp trên bảng ổ nối tăng từ sáu lên mười dây. Thay vì chỉ có mười hai chữ cái được hoán đổi trước khi đi vào các đĩa

mã hóa thì nay có tới hai mươi chữ cái. Số khóa mã tiềm năng tăng lên đến 159.000.000.000.000.000.000.

Bảng 10 Các cách sắp xếp có thể với năm đĩa mã hóa

Các cách sắp đặt với 3 đĩa mã hóa	Các cách sắp đặt thêm với hai đĩa mã hóa bổ sung								
123	124	125	134	135	142	143	145	152	153
132	154	214	215	234	235	241	243	245	251
213	253	254	314	315	324	325	341	342	345
231	351	352	354	412	413	415	421	423	425
312	431	432	435	451	452	453	512	513	514
321	521	523	524	531	532	534	541	542	543

Năm 1938, lượng thông tin mà người Ba Lan chặn bắt và giải mã được đã lên đến đỉnh điểm của nó nhưng đến đầu năm 1939, các đĩa mã hóa mới và dây cáp bổ sung thêm vào bảng ổ nối đã chặn đứng lại dòng thông tin tình báo. Rejewski, người đã từng đẩy xa hơn ranh giới của việc giải mã trong những năm trước đây, nay cũng bị đánh bại. Ông đã chứng minh được rằng Enigma không phải là một mật mã không thể giải mã được, nhưng nếu không có những cơ sở cần thiết để kiểm tra mỗi cách sắp đặt các đĩa mã hóa thì ông cũng không thể tìm ra khóa mã ngày, và do đó việc giải mã là không thể thực hiện được. Trước tình thế tuyệt vọng này, Langer hẳn buộc phải đưa ra các khóa mã có được từ Schmidt, song các khóa mã này không còn được gửi đến nữa. Ngay trước khi có thêm các đĩa mã hóa mới, Schmidt đã cắt đứt liên lạc với điệp viên Rex. Trong suốt bảy năm, ông ta đã cung cấp các khóa mã nhưng chúng lại vô dụng vì phát minh

của người Ba Lan. Giờ đây, đúng lúc mà người Ba Lan cần đến khóa mã thì lại không thể có được nữa.

Khả năng không thể xâm phạm mới này của Enigma như một cơn chấn động mạnh đối với Ba Lan vì Enigma không chỉ là một phương tiện liên lạc mà còn là trái tim trong chiến lược *blitzkrieg* của Hitler. Khái niệm blitzkrieg (chiến tranh chớp nhoáng) có nghĩa là tấn công nhanh, mạnh và hợp đồng binh chủng, tức là các sư đoàn xe tăng lớn sẽ phải liên lạc với nhau và với cả bộ binh và pháo binh. Hơn nữa, các lực lượng trên mặt đất sẽ được yểm trợ từ trên không bởi các máy bay tiêm kích ném bom bổ nhào Stukas, mà điều này thì phụ thuộc vào hiệu quả và mức độ an toàn trong thông tin liên lạc giữa các đơn vị ở tuyến trước và trên không. Đặc trưng của blitzkrieg đó là "tốc độ tấn công thông qua tốc độ thông tin liên lạc". Nếu người Ba Lan không thể phá vỡ Enigma, họ không có hy vọng gì ngăn chặn được những cuộc tấn công bất ngờ của người Đức, mà điều này thì chỉ là vấn đề tính bằng tháng. Vì giờ đây, Đức đã chiếm đóng Sudetenland, và đã hủy bỏ hiệp ước không xâm phạm lãnh thổ của nhau với Ba Lan ngày 27 tháng Tư năm 1939. Nhưng lời lẽ tuyên truyền chống Ba Lan của Hitler ngày càng trở nên cay độc. Langer quyết định rằng nếu Ba Lan bị xâm lược thì những tiến bộ về giải mã của họ, cho đến lúc này vẫn còn giữ bí mật đối với quân Đồng minh, không thể để bị thất lạc. Nếu Ba Lan không được hưởng lợi ích từ thành quả của Rejewski thì ít nhất quân Đồng minh cũng phải có cơ hội để thử và thực hiện nó. Có thể là Anh và Pháp, với những tiềm lực trội hơn, sẽ khai thác được đầy đủ khái niệm về *bom*.

Ngày 30 tháng Sáu, thiếu tá Langer đã gửi điện cho các đồng nghiệp người Anh và Pháp của mình, mời họ tới Vácsava để thảo

luận về một số vấn đề khẩn cấp liên quan đến Enigma. Ngày 24 tháng Bảy, các nhà giải mã cấp cao của Anh và Pháp đã có mặt tại trụ sở chính của Biuro, nhưng không hoàn toàn biết về những gì sẽ thảo luận. Langer đưa họ vào một căn phòng, bên trong chỉ có một vật được che bằng một tấm vải màu đen. Ông kéo tấm vải xuống và trước mắt họ là một trong những máy *bom* của Rejewski. Toàn bộ cử tọa rất kinh ngạc khi nghe kể về việc Rejewski đã giải mã Enigma từ những năm trước như thế nào. Người Ba Lan đã đi trước tất cả những người khác trên thế giới cả một thập kỷ. Người Pháp thì đặc biệt kinh ngạc, vì thành tựu của người Ba Lan là dựa trên kết quả tình báo của Pháp. Người Pháp đã trao những thông tin có được từ Schmidt cho người Ba Lan vì họ tin rằng nó chẳng có giá trị gì, song người Ba Lan đã chứng minh rằng họ đã lầm.

Hình 43 Chiếc xe điện đài chỉ huy của tướng Heinz Guderian. Chúng ta có thể thấy một chiếc Enigma đang được sử dụng ở góc dưới bên trái.

Điều ngạc nhiên cuối cùng là Langer đã tặng người Anh và Pháp hai bản sao máy Enigma và bản thiết kế *bom*, sẽ được gửi bằng tàu biển qua con đường ngoại giao tới Paris. Từ đây, ngày 16

tháng Tám, một trong hai máy Enigma đó sẽ được chuyển tới London. Nó được mang lậu qua eo biển Măngsơ dưới dạng hành lý của cặp vợ chồng nhà viết kịch Sacha Guitry và nữ diễn viên Yvonne Printemps, và vì vậy đã không gây bất kỳ sự nghi ngờ nào của các điệp viên Đức theo dõi các bến cảng. Hai tuần sau đó, vào ngày 1 tháng Chín, Hitler đã tấn công Ba Lan và cuộc chiến tranh bắt đầu.

Con ngỗng không bao giờ kêu quạc quạc

Trong mười ba năm, Anh và Pháp đã cho rằng mật mã Enigma là không thể hóa giải được, nhưng giờ đây đã có hy vọng. Những phát hiện của người Ba Lan chứng minh rằng mật mã Enigma cũng có sơ hở, nhờ đó đã khích lệ tinh thần các nhà giải mã của quân Đồng minh. Sự tiến triển của người Ba Lan bị tạm dừng vì có thêm hai đĩa mã hóa mới và các dây cáp bên trong bảng ổ nối, song sự thực là Enigma giờ đây đã không còn được coi là một loại mật mã hoàn hảo nữa.

Thành tựu của người Ba Lan cũng chứng minh cho quân Đồng minh thấy giá trị của việc sử dụng các nhà toán học như là các nhà giải mã. Ở Anh, Phòng 40 chủ yếu chỉ có các nhà ngôn ngữ và các chuyên gia ngôn ngữ cổ, nhưng giờ đây đã có một nỗ lực phối hợp nhằm cân bằng cơ cấu giữa các nhà toán học và các nhà khoa học. Họ được tuyển dụng phần lớn thông qua hệ thống bạn học cũ với những người làm việc tại Phòng 40, liên lạc thông qua các trường học cũ của họ ở Oxford và Cambridge. Cũng có cả hệ thống các bạn học cũ là nữ giới, nhằm tuyển dụng những người đã từng tốt nghiệp từ các trường như Newham và Girton thuộc Cambridge.

Những người mới được tuyển dụng này không được đưa tới Phòng 40 ở London mà thay vào đó là Bletchley Park, ở Buckinghamshire, ngôi nhà của Trường Mật mã của Chính phủ (GC&CS), một tổ chức về giải mã mới kế tục Phòng 40. Bletchley Park có thể chứa được số người lớn hơn, điều này là rất quan trọng vì người ta cho rằng ngay khi chiến tranh nổ ra thì lượng thư từ mã hóa chặn bắt được sẽ đến dồn dập. Trong suốt Thế chiến Thứ nhất, người Đức đã truyền đi hai triệu từ trong một tháng, song người ta dự đoán rằng với sự tràn ngập của liên lạc vô tuyến trong Thế chiến Thứ hai thì sẽ phải là hai triệu từ một ngày.

Trung tâm của Bletchley Park là một tòa lâu đài lớn được xây dựng vào thế kỷ 19 theo kiểu Tudor-Gothic thời Victoria do Ngài Herbert Leon tài trợ. Tòa lâu đài, với thư viện, phòng ăn tối và

Hình 44 Tháng Tám năm 1939, các nhà giải mã cấp cao của Anh đã đến Bletchley Park để xem xét sự thích hợp của nó cho vị trí của Trường Mật mã của Chính phủ mới được thành lập. Để tránh gây sự chú ý của người dân địa phương, họ giả làm thành viên hội bắn súng của Đại úy Ridley.

phòng khiêu vũ lộng lẫy, là nơi điều hành trung tâm đối với toàn bộ hoạt động ở Bletchley. Chỉ huy ở đây là Alastair Denniston, giám đốc GC&CS, có văn phòng làm việc ở tầng một nhìn ra vườn, một quang cảnh mà chẳng mấy chốc đã bị làm hỏng bởi một loạt các nhà tạm mọc lên ở đó. Những căn nhà làm bằng gỗ tạm thời này được dùng cho các hoạt động giải mã khác nhau. Chẳng hạn, Nhà số 6 chuyên tấn công mạng lưới thông tin dùng Enigma của quân đội Đức. Nhà số 6 chuyển các bản giải mã đến cho Nhà số 3, tại đây các chuyên gia tình báo sẽ dịch thư từ và tìm cách khai thác thông tin. Nhà số 8 tập trung vào Enigma hải quân và họ chuyển các bản giải mã qua Nhà số 4 để dịch và thu thập thông tin tình báo. Ban đầu, Bletchley Park chỉ có khoảng hai trăm nhân viên, nhưng trong vòng năm năm thì tòa lâu đài và các nhà tạm đã chứa đến bảy ngàn người cả nam lẫn nữ.

Suốt cả mùa thu năm 1939, các nhà khoa học và toán học ở Bletchley đã tập trung tìm hiểu tất cả các khía cạnh phức tạp của mật mã Enigma và họ đã nhanh chóng làm chủ các kỹ thuật của người Ba Lan. Bletchley có số lượng nhân viên và tiềm lực mạnh hơn Biuro Szyfrów và vì vậy có thể đối phó được với việc có nhiều hơn các đĩa mã hóa và sự thực thì Enigma lúc này đã khó hóa giải hơn gấp mười lần. Cứ mỗi 24 giờ, các nhà giải mã Anh đều phải hoàn tất cùng một thủ tục. Vì đúng nửa đêm, những người vận hành máy Enigma của Đức lại thay đổi sang khóa mã ngày mới, lúc đó những kết quả mà Bletchley đạt được của ngày hôm trước lại không thể sử dụng để giải mã được nữa. Lúc này họ lại bắt đầu nhiệm vụ xác định khóa mã ngày mới. Việc này có thể mất khoảng vài giờ, nhưng ngay khi họ khám phá ra cách sắp đặt của máy Enigma ngày hôm đó, thì các nhân

viên Bletchley có thể bắt đầu giải mã thư từ của quân Đức đến mỗi lúc một tăng, các thông tin khám phá ra là vô giá đối với nỗ lực chiến tranh.

Bất ngờ là một vũ khí vô giá cho người chỉ huy cần phải có trong tay. Nhưng nếu Bletchley có thể hóa giải Enigma, thì các kế hoạch của Đức sẽ trở nên "trong suốt" và người Anh có thể đọc được những toan tính của Tổng hành dinh Tối cao của Đức. Nếu người Anh có thể thu thập tin tức về một cuộc tấn công sắp xảy đến, họ có thể gửi quân chi viện hoặc có hành động tấn công trước. Nếu họ có thể giải mã được những cuộc thảo luận của Đức về những điểm yếu của họ thì quân Đồng minh có thể tập trung vào việc phòng thủ. Sự giải mã của Bletchley là cực kỳ quan trọng. Chẳng hạn, khi Đức tấn công Đan Mạch và Na Uy vào tháng Tư năm 1940, Bletchley đã cung cấp một bức tranh chi tiết về hành động của Đức. Tương tự như vậy, trong suốt cuộc chiến của Anh, các nhà giải mã đã cung cấp những cảnh báo trước về cuộc tấn công bằng bom, cả về thời gian lẫn địa điểm. Họ cũng có thể cung cấp những thông tin cập nhật tiếp theo về tình hình của *Luftwaffe* (không lực), chẳng hạn như số máy bay đã bị mất tích và tốc độ thay thế chúng. Bletchley gửi tất cả các thông tin này đến các trụ sở của MI6, và tổ chức này sẽ chuyển tiếp đến Bộ Quốc phòng, Bộ Không quân và Bộ Hải quân.

Giữa những thời gian tác động đến diễn tiến của cuộc chiến tranh, các nhà giải mã cũng tìm được những thời khắc hiếm hoi để thư giãn. Theo Malcolm Muggeridge, người làm việc trong cơ quan mật vụ và đã từng tới thăm Bletchley, thì trò chơi bóng bằng vợt, một dạng bóng mềm, là một trò tiêu khiển được họ ưa thích:

Mỗi ngày sau bữa trưa, khi thời tiết thuận lợi, các nhà giải mã chơi bóng mềm bằng vợt trên bãi cỏ trong vườn của trang viên. Họ vẫn mang dáng vẻ khá đạo mạo do ảnh hưởng của những ông thầy ở các trường Đại học Oxford hoặc Cambridge danh tiếng ngay cả khi tham gia các hoạt động được coi như là tầm phào hoặc không đáng kể gì so với những nghiên cứu nặng nề của họ. Họ tranh luận về một số điểm của trò chơi bóng này cũng hăng say như khi họ tranh luận về ý chí tự do hay quyết định luận, hoặc liệu thế giới có phải bắt đầu bằng một Vụ nổ lớn không hay đó là một quá trình sáng tạo liên tục.

Khi đã làm chủ được kỹ thuật của người Ba Lan, những nhà giải mã ở Bletchley bắt đầu tìm ra những con đường tắt của riêng mình để tìm ra chìa khóa mã của Enigma. Chẳng hạn, họ đã chú ý đến một thực tế là những người điều khiển máy Enigma người

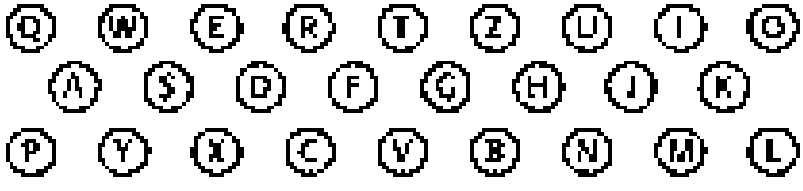
Hình 45. Các nhà giải mã Bletchley thư giãn với trò chơi bóng bằng vợt.

Đức thường lựa chọn các khóa mã thư một cách không mấy phức tạp. Với mỗi bức thư, người điều khiển được quyền lựa chọn một khóa mã thư khác chứa ba chữ cái ngẫu nhiên. Tuy nhiên, trong thời điểm nóng bỏng của cuộc chiến, thay vì ép buộc trí tưởng tượng phải chọn ra một chìa khóa mã ngẫu nhiên, những người điều khiển làm việc quá nhiều đôi khi sẽ chọn ngay những chữ cái liền nhau trên bàn phím của máy Enigma (Hình 46), chẳng hạn như **QWE** hay **BNM**. Những khóa mã thư có thể dự đoán trước được này gọi là các *cilly*. Một dạng khác của *cilly* đó là việc sử dụng lặp lại cùng một khóa mã thư, có thể đó là các chữ cái đầu trong tên người bạn gái của người điều khiển máy - thực sự thì đã có một nhóm các chữ cái đầu như vậy, đó là C.I.L, và có thể đây chính là xuất xứ của từ *cilly*. Trước khi hóa giải Enigma theo con đường phức tạp hơn thì việc thử *cilly* đã trở thành một thói quen của các nhà giải mã và đôi khi những linh cảm của họ cũng mang lại kết quả tốt.

Cilly không phải là điểm yếu của Enigma, mà chỉ là điểm yếu trong cách thức sử dụng máy. Sai lầm của con người ở trình độ cao hơn cũng gây tổn hại đến sự an toàn của mật mã Enigma. Nhưng trách nhiệm này nằm ở việc soạn thảo sổ mã, trong đó quyết định đến đĩa mã hóa nào được sử dụng mỗi ngày và vị trí của chúng. Họ cố gắng bảo đảm để sự sắp đặt đĩa mã hóa là không thể dự đoán trước được bằng cách không cho phép bất kỳ đĩa mã hóa nào được ở cùng một vị trí trong hai ngày liền. Vì vậy, nếu chúng ta đánh số các đĩa mã hóa là 1, 2, 3, 4 và 5, thì trong ngày đầu tiên, cách sắp xếp có thể là 134, ngày thứ hai có thể là 215, chứ không thể là 214, vì đĩa mã hóa số 4 không được phép ở cùng một vị trí trong hai ngày liền. Đây có vẻ như

là một chiến lược khôn ngoan vì các đĩa mã hóa thay đổi vị trí một cách đều đặn, song việc bắt buộc tuân thủ một quy tắc như vậy thực sự làm cho cuộc sống của các nhà giải mã dễ chịu hơn. Việc loại trừ những sắp xếp nhất định để tránh việc một đĩa mã hóa vẫn ở vị trí cũ có nghĩa là những người soạn sổ mã giảm đi một nửa số cách sắp xếp có thể của các đĩa mã hóa. Các nhà giải mã ở Bletchley đã nhận ra điều này và tận dụng nó. Một khi họ xác định được sự sắp xếp các đĩa mã hóa ngày hôm đó thì họ có thể ngay lập tức tìm ra nửa số cách sắp xếp còn lại của ngày tiếp theo. Do vậy, lượng công việc của họ giảm đi một nửa.

Tương tự, có một quy tắc nữa đó là sự cài đặt bảng ổ nối cũng không thể bao gồm việc hoán đổi giữa hai chữ cái nằm cạnh nhau, tức là **S** có thể được nối với bất kỳ chữ cái nào khác ngoại trừ **R** và **T**. Quy tắc này buộc người ta phải chủ tâm tránh dùng một số hoán đổi, song lại một lần nữa, việc thực hiện triệt để một nguyên tắc lại làm giảm số các chìa khóa mã tiềm năng.



Hình 46 Sơ đồ bàn phím máy Enigma

Việc tìm kiếm những con đường tắt mới để giải mã này là cần thiết vì máy Enigma liên tục được cải tiến trong suốt tiến trình của cuộc chiến. Các nhà giải mã vẫn tiếp tục bị buộc phải cải tiến, thiết kế lại và nâng cấp máy *bom* và lập ra những chiến lược hoàn toàn mới. Một phần lý do dẫn tới thành công của họ chính là sự kết hợp lạ lùng giữa các nhà toán học, khoa học, ngôn ngữ học,

các kiện tướng cờ vua và những người nghiền chơi ô chữ trong các ngôi nhà tạm. Một vấn đề nan giải có thể được chuyển quanh cho đến khi ai đó có khả năng giải quyết nó hoặc đến một ai đó có thể ít nhất giải quyết được một phần trước khi chuyển tiếp cho những người khác. Gordon Welchman, người phụ trách Nhà số 6, đã mô tả nhóm của mình như là "một bầy chó săn tìm mọi cách đánh hơi". Có rất nhiều nhà giải mã vĩ đại và nhiều thành tựu to lớn, và sẽ phải cần đến nhiều chương mới mô tả được hết đóng góp của từng người. Tuy nhiên, nếu có một nhân vật đáng được nói riêng đến thì đó chính là Alan Turing, người đã xác định được điểm yếu lớn nhất của máy Enigma và đã tận dụng nó một cách triệt để. Nhờ có Turing mà người ta đã có thể giải được mật mã Enigma ngay cả dưới những điều kiện khó khăn nhất.

Mẹ của Alan Turing mang thai ông vào mùa thu năm 1911 ở Chatrapur, một thị trấn gần Madras miền nam Ấn Độ, nơi cha ông, Julius Turing, là một công chức hành chính dân sự. Julius và vợ là Ethel đã quyết định sinh cậu con trai ở Anh và quay trở về London, và Alan đã ra đời vào ngày 23 tháng Bảy năm 1912. Cha ông quay lại Ấn Độ ngay sau đó và 15 tháng sau mẹ ông cũng đi theo, để Alan lại cho những người vú em và bạn bè chăm sóc cho đến khi cậu đủ lớn để có thể đi học ở trường nội trú.

Năm 1926, ở tuổi 14, Turing vào học tại trường Sherborne ở Dorset. Học kỳ của cậu bắt đầu đồng thời với cuộc Tổng bãi công xảy ra, song Turing vẫn quyết định tới dự buổi học đầu tiên, và cậu đã một mình đạp xe trên 100km từ Southampton đến Sherborne. Chiến công này đã được đưa tin trên báo địa phương. Đến cuối năm học đầu tiên ở trường, cậu đã nổi tiếng là một học sinh nhút nhát, vụng về nhưng lại rất có năng lực trong lĩnh vực

khoa học. Mục tiêu của trường Sherborne là biến học sinh của họ thành những người đàn ông có hiểu biết rộng, thích hợp để lãnh đạo Đế chế, song Turing không muốn chia sẻ tham vọng này và nói chung là cậu đã có một thời đi học không mấy vui vẻ.

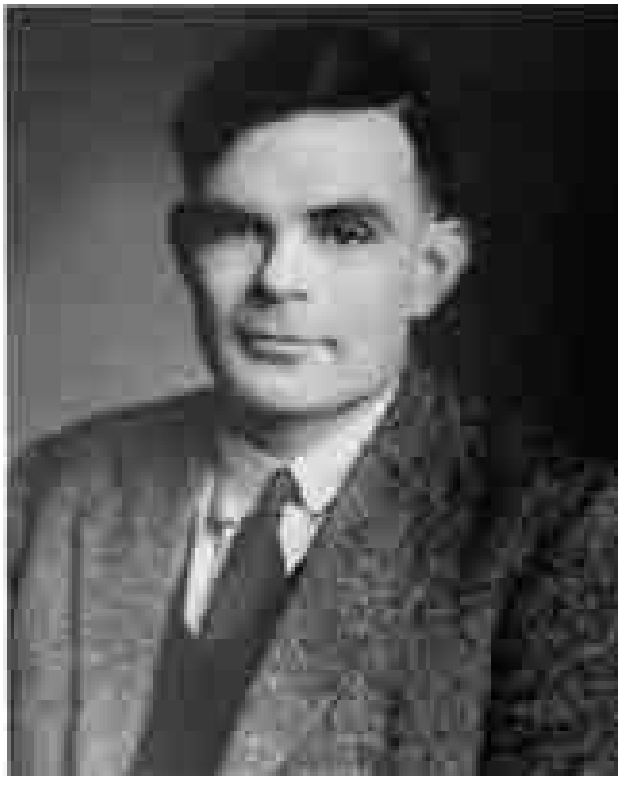
Người bạn duy nhất của cậu ở Sherborne là Christopher Morcom, người cũng giống như Turing, chỉ quan tâm đến khoa học. Họ đã cùng nhau thảo luận về những thông tin khoa học mới nhất và tự tiến hành các thí nghiệm. Mối quan hệ này đã khơi lên trong Turing sự tò mò trí tuệ, nhưng, quan trọng hơn, nó đã có một ảnh hưởng tình cảm sâu sắc đối với ông. Andrew Hodges, người viết tiểu sử của Turing, đã viết rằng "Đây là mối tình đầu... Nó mang cái cảm giác buông xuôi cho cám dỗ ấy, cùng một tri giác thăng hoa, dường như sắc màu rực rỡ đã nổ bùng ra trong một thế giới hai màu đen trắng". Mối quan hệ của họ kéo dài trong bốn năm, nhưng Morcom dường như không nhận ra chiều sâu tình cảm mà Turing dành cho mình. Sau đó, vào năm cuối cùng của họ ở Sherborne, Turing đã vĩnh viễn mất cơ hội để nói với Morcom về tình cảm của mình. Vào thứ Năm, ngày 13 tháng Hai năm 1930, Christopher Morcom đã mất đột ngột vì bệnh lao phổi.

Turing đã rất đau khổ vì mất đi một người duy nhất mà cậu đã thực sự yêu mến. Cách duy nhất để nguôi ngoai về cái chết của Morcom đó là tập trung vào học những môn khoa học với mong muốn thực hiện tâm nguyện của bạn mình. Morcom, dường như có năng khiếu hơn trong hai người, đã giành được một học bổng của trường Đại học Cambridge. Turing tin rằng trách nhiệm của cậu là phải giành được một vị trí ở Cambridge, và sau đó là phải tiến hành những khám phá mà lẽ ra bạn của cậu sẽ làm. Cậu xin mẹ của Christopher một bức ảnh và khi nhận được, cậu đã viết

thư cảm ơn bà: "Giờ anh ấy đang ở trên bàn của cháu, động viên cháu làm việc thật chăm chỉ".

Năm 1931, Turing đã được nhận vào học tại trường King's College, Cambridge. Ông đến đúng vào thời kỳ đang diễn ra những tranh cãi gay gắt về bản chất của toán học và logic, với những tiếng nói đầy uy tín của Bertrand Russell, Alfred North Whitehead và Ludwig Wittgenstein. Trung tâm của cuộc tranh cãi là vấn đề về *tính không thể quyết định*, một khái niệm gây tranh cãi do nhà logic học Kurt Gôdel đề xướng. Người ta luôn luôn cho rằng, ít nhất là về mặt lý thuyết, tất cả các vấn đề toán học đều có thể giải đáp được. Tuy nhiên, Gôdel đã chứng minh rằng có tồn tại một số ít các vấn đề vượt ra ngoài tầm của chứng minh logic, chúng được gọi là những vấn đề không thể quyết định được. Các nhà toán học đã bị sốc trước thông tin nói rằng toán học không phải là một môn học toàn năng như họ vẫn hằng tin như vậy. Họ toan tính bảo vệ môn học của mình bằng cách cố tìm ra một phương cách để xác định những vấn đề kỳ quặc không thể quyết định được, từ đó họ có thể an tâm gạt chúng qua một bên. Chủ đề này cuối cùng đã gợi cảm hứng cho Turing viết một bài báo có ảnh hưởng lớn nhất của ông về toán học, *Về những con số tính toán được*, được công bố năm 1937. Trong *Giải mã*, một vở kịch của Hugh Whitemore nói về cuộc đời của Turing, một nhân vật đã hỏi Turing về ý nghĩa của bài báo đó. Ông trả lời, "Nó viết về đúng và sai. Nói một cách tổng quát, đây là một bài báo chuyên môn về logic toán, song nó cũng nói về sự khó khăn trong việc phân biệt đúng và sai. Mọi người - hay đúng hơn là hầu hết mọi người - nghĩ rằng trong toán học chúng ta luôn biết rõ cái gì là đúng và cái gì là sai. Nhưng không phải như vậy. Và không còn như vậy nữa."

Trong nỗ lực nhằm xác định những vấn đề không thể quyết định được, bài báo của Turing đã mô tả một cỗ máy tưởng tượng được thiết kế để thực hiện một phép tính toán học cụ thể, hay một thuật toán. Nói cách khác, cỗ máy này có thể chạy qua một chuỗi những bước đã định sẵn để, chẳng hạn, nhân hai số với nhau. Turing đã mường tượng rằng các số sẽ được nhân với nhau có thể được nạp vào máy qua một băng giấy, giống như băng giấy đục lỗ được sử dụng để nạp âm vào một chiếc máy chơi nhạc tự động. Đáp số của phép nhân sẽ đi ra qua một băng giấy khác. Turing đã tưởng tượng ra một loạt các máy được gọi là *Máy Turing*, mỗi cái được thiết kế đặc biệt để thực hiện một nhiệm vụ riêng biệt, chẳng hạn như phép chia, phép khai căn hoặc lấy giai thừa. Sau đó Turing đã thực hiện một bước cơ bản hơn.



Alan Turing

Ông tưởng tượng ra một cỗ máy mà sự vận hành bên trong nó có thể thay đổi, nhờ đó, nó có thể thực hiện được tất cả các chức năng của tất cả các máy Turing. Những thay đổi sẽ được thực hiện bằng cách đưa vào những băng giấy được lựa chọn một cách thận trọng, nhờ đó có thể chuyển đổi được một cỗ máy linh hoạt duy nhất thành máy chia, máy nhân hay bất kỳ loại máy nào khác. Turing gọi thiết bị giả tưởng này là *máy Turing vạn năng* vì

nó có khả năng giải đáp mọi câu hỏi mà về mặt logic có thể trả lời được. Thật không may, người ta đã chỉ ra rằng không phải bao giờ về mặt logic cũng có thể trả lời được câu hỏi về tính không thể quyết định được của một câu hỏi khác, và vì vậy ngay cả máy vạn năng của Turing cũng không thể xác định được tất cả các câu hỏi không thể quyết định được.

Sau khi đọc bài báo của Turing, các nhà toán học đã thất vọng rằng con quái vật của Gôdel đã không bị thuần phục nhưng, như là một niềm an ủi, Turing lại mang đến cho họ một bản thiết kế chi tiết của chiếc máy tính hiện đại có thể lập trình được. Turing đã biết đến công trình của Babbage và máy Turing vạn năng có thể xem như một sự hồi sinh của Máy Sai phân số 2. Trong thực tế, Turing đã tiến xa hơn nhiều, ông đã mang lại cho sự tính toán một cơ sở lý thuyết chắc chắn, làm cho máy tính đó có một tiềm năng không thể tưởng tượng được cho đến nay. Đó mới chỉ là vào những năm 1930 và công nghệ vẫn chưa tồn tại để biến máy Turing vạn năng trở thành hiện thực. Song, Turing không hề thất vọng vì lý thuyết của mình đã đi trước cả những gì khả thi về mặt công nghệ. Ông chỉ muốn có được sự thừa nhận từ bên trong cộng đồng toán học, những người đã thực sự tán thưởng bài báo của ông như là một trong những đột phá quan trọng nhất của thế kỷ. Lúc đó ông mới chỉ có 26 tuổi.

Đó là một thời kỳ hạnh phúc và thành công đặc biệt đối với Turing. Trong suốt những năm 1930, ông đã liên tục được thăng tiến qua các cương vị để trở thành một thành viên của trường King's College, ngôi nhà chung của những bộ não ưu tú nhất thế giới. Ông đã sống cuộc đời điển hình của một giáo sư trường Cambridge, một cuộc sống kết hợp toán học thuần túy với những

hoạt động bình thường hơn. Năm 1938, ông đã đi xem phim *Nàng Bạch Tuyết và Bảy chú lùn*, trong đó có một cảnh đáng nhớ là Mụ phù thủy Độc ác nhúng quả táo vào thuốc độc. Sau đó, đồng nghiệp của ông đã nghe thấy Turing hát đi hát lại câu "Nhúng quả táo vào rượu, Để cho cái chết lịm dần thấm qua".

Turing đã rất yêu quý những năm ở Cambridge. Ngoài những thành công trong khoa học, ông còn được sống trong một môi trường đầy sự động viên và độ lượng. Đồng tính được chấp nhận rộng rãi trong trường đại học này và điều đó có nghĩa là ông được thoải mái trong các mối quan hệ mà không phải lo sợ có người biết và người khác nói gì. Tuy ông không có một mối quan hệ kéo dài và nghiêm túc nào, song ông dường như hài lòng với cuộc sống của mình. Sau đó, vào năm 1939, sự nghiệp khoa học của Turing đã dừng lại một cách đột ngột. Trường Mật mã của Chính phủ đã mời ông đến làm một nhà giải mã tại Bletchley và ngày 4 tháng Chín năm 1939, một ngày sau khi Neville Chamberlain tuyên bố chiến tranh với Đức, Turing đã chuyển từ khuôn viên sang trọng của trường Cambridge đến Quán trọ Crown ở Shenley Brook End.

Mỗi ngày, ông đạp xe 5 km từ Shenley Brook End đến Bletchley Park, nơi ông dành một phần thời gian của mình góp phần vào nỗ lực giải mã thường lệ trong các nhà tạm, và một phần thời gian vào bộ phận chuyên gia, ở chỗ trước đây là hầm chứa táo, lê và mận của Ngài Herbert Leon. Bộ phận chuyên gia là nơi các nhà giải mã có những sáng kiến bất chợt về cái cách mà họ vượt qua những vấn đề mới, hay dự kiến trước cách giải quyết những vấn đề có thể sẽ nảy sinh trong tương lai. Turing tập trung vào những gì sẽ xảy ra nếu quân đội Đức thay đổi hệ thống trao đổi chìa khóa mã thư của họ. Những thành công bước đầu của

Bletchley dựa trên thành quả của Rejewski, tận dụng thực tế là những người điều khiển máy Enigma đã mã hóa mỗi khóa mã thư hai lần (ví dụ, nếu khóa mã thư là **YGB**, thì người điều khiển sẽ mã hóa **YGBYGB**). Sự lặp lại này là nhằm bảo đảm để người nhận không bị nhầm lẫn, nhưng nó lại tạo ra một kẽ hở trong sự an toàn của Enigma. Các nhà giải mã Anh đoán rằng nó sẽ không kéo dài trước khi người Đức nhận ra rằng khóa mã lặp lại đã làm tổn hại đến mật mã Enigma, lúc đó những người điều khiển Enigma sẽ được chỉ thị không được lặp lại và do đó sẽ vô hiệu hóa kỹ thuật giải mã hiện tại của Bletchley. Nhiệm vụ của Turing chính là tìm ra một cách khác để tấn công Enigma, một cách mà nó không phụ thuộc vào khóa mã thư lặp lại.

Vài tuần trôi qua, Turing nhận thấy Bletchley đã tích tụ được một thư viện với khối lượng cực lớn các bức thư được giải mã, và ông thấy rằng rất nhiều trong số đó đều tuân theo một cấu trúc chặt chẽ. Bằng cách nghiên cứu những bức thư đã được giải mã cũ, ông tin rằng đôi khi có thể dự đoán được một phần nội dung của một bức thư chưa được giải mã, dựa trên dữ liệu khi nào nó được gửi đến và gửi đến từ đâu. Chẳng hạn, kinh nghiệm cho thấy người Đức gửi một báo cáo thời tiết được mã hóa đều đặn ngay sau 6 giờ sáng mỗi ngày. Vì vậy, một bức thư mã hóa chặn bắt được vào lúc 6h05 sáng sẽ gần như chắc chắn có từ **wetter**, tiếng Đức có nghĩa là "thời tiết". Thủ tục nghiêm ngặt được sử dụng bởi bất kỳ một tổ chức quân đội nào có nghĩa là những bức thư kiểu này bao giờ cũng được viết theo một khuôn mẫu nhất định, do vậy Turing có thể tự tin chỉ ra vị trí của từ **wetter** trong các bức thư được mã hóa. Chẳng hạn, kinh nghiệm cho ông biết rằng sáu chữ cái đầu tiên của một đoạn mật mã cụ thể nào đó sẽ

tương ứng với từ **wetter** trong văn bản thường. Khi một đoạn văn bản thường có thể gắn với một đoạn văn bản mật mã, thì sự kết hợp này được gọi là một *crib* (nghĩa đen là *bản dịch sát từng chữ).*

Turing chắc chắn rằng ông có thể tận dụng các *crib* này để hóa giải Enigma. Nếu ông đã có một văn bản mật mã và ông biết chắc một đoạn của nó, chẳng hạn **ETJWPX**, là mã hóa của **wetter**, thì vấn đề đặt ra là xác định cách cài đặt máy Enigma sao cho nó chuyển đổi **wetter** thành **ETJWPX**. Cách đơn giản, nhưng phi thực tế, để thực hiện việc này, đó là các nhà giải mã sử dụng một máy Enigma, đánh vào **wetter** và xem văn bản mật mã hiện ra có đúng không. Nếu không, nhà giải mã lại thay đổi cách cài đặt của máy, bằng cách hoán đổi các dây nối trong bảng ổ nối, và hoán đổi hoặc đổi định hướng của các đĩa mã hóa, và sau đó đánh lại **wetter** lần nữa. Nếu kết quả đúng vẫn chưa hiện ra, nhà giải mã sẽ lại thay đổi cách cài đặt một lần nữa, và lần nữa và cứ tiếp tục như vậy cho đến khi anh ta nhận được một kết quả đúng. Vấn đề duy nhất gặp phải ở đây với cách tiếp cận thử và sai nói trên, đó là thực tế có tới 159.000.000.000.000.000.000 cách cài đặt tiềm năng cần kiểm tra, do vậy việc tìm ra cách cài đặt chuyển đổi **wetter** thành **ETJWPX** dường như là một nhiệm vụ bất khả thi.

Để đơn giản hóa vấn đề này, Turing đã thử làm theo chiến lược gỡ riêng các cách cài đặt ra của Rejewski. Ông muốn tách riêng việc tìm các cách sắp đặt các đĩa mã hóa (tức là tìm ra đĩa mã hóa nào nằm ở khe nào, và các định hướng tương ứng của chúng) và việc tìm các dây nối trong bảng ổ nối. Chẳng hạn, nếu ông có thể tìm thấy điều gì đó ở *crib* mà không liên quan gì đến các dây trong bảng ổ nối thì ông có thể kiểm tra được tất cả 1.054.560 khả năng kết hợp giữa các đĩa mã hóa (60 cách sắp xếp

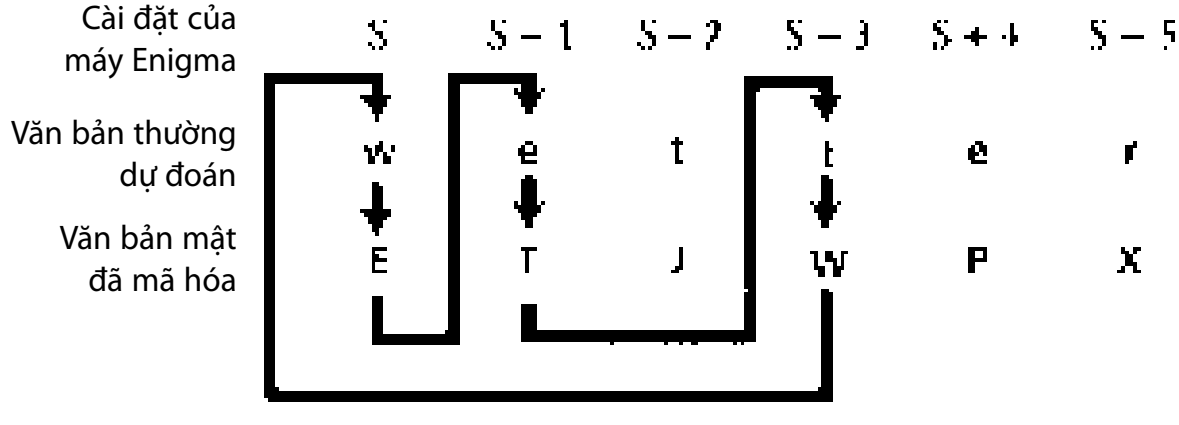
× 17.576 hướng). Khi tìm thấy cách sắp đặt đúng, ông có thể xác định được cách nối dây trong ổ nối.

Cuối cùng, ông tập trung vào một dạng *crib* cụ thể, trong đó có chứa các vòng, tương tự như các vòng của Rejewski. Các vòng của Rejewski liên kết các chữ cái trong khóa mã thư lặp lại. Tuy nhiên, các vòng của Turing lại không liên quan gì đến khóa mã thư, vì ông đang làm việc dựa trên giả định rằng sớm muộn người Đức cũng sẽ dừng việc gửi các khóa mã thư lặp lại. Thay vào đó, các vòng của Turing nối các chữ cái trong văn bản thường và văn bản mật mã của một *crib*. Chẳng hạn, *crib* trong Hình 48 có chứa 1 vòng.

Hãy nhớ rằng các *crib* chỉ là dự đoán, nhưng nếu chúng ta giả sử rằng *crib* này là đúng thì chúng ta có thể liên kết các chữ cái **w** → **E**, **e** → **T**, **t** → **W** như là các bộ phận của một vòng. Tuy chúng ta không biết sự cài đặt nào của Enigma, nhưng chúng ta có thể gọi cài đặt đầu tiên, bất kể nó là thế nào, là **S**. Trong cài đặt đầu tiên này, chúng ra biết rằng **w** được mã hóa thành **E**. Sau khi mã hóa xong, đĩa mã hóa thứ nhất dịch đi một vị trí, chuyển sang cài đặt S+1, và chữ cái **e** được mã hóa thành **T**. Đĩa mã hóa này lại dịch đi một vị trí nữa và mã hóa một chữ cái không phải là một bộ phận của vòng, vì vậy chúng ta bỏ qua sự mã hóa này. Đĩa mã hóa dịch đi một vị trí nữa và, một lần nữa, chúng ta đến chữ cái **t** là một bộ phận của vòng. Ở cài đặt S+3, chúng ta biết rằng chữ cái **t** được mã hóa thành **W**. Tóm tắt lại, chúng ta biết rằng

ở cài đặt S,	Enigma mã hóa	**w** thành **E**
ở cài đặt S+1,	Enigma mã hóa	**e** thành **T**
ở cài đặt S+3,	Enigma mã hóa	**t** thành **W**

Đến lúc này thì vòng dường như chẳng gì khác hơn là một khuôn mẫu gợi sự tò mò, song Turing đã theo dõi sát sao những **ngụ ý** của các mối quan hệ bên trong của vòng, và thấy rằng chúng mang lại cho ông một con đường tắt rất quan trọng mà ông cần để hóa giải Enigma. Thay vì làm việc với chỉ một máy Enigma để kiểm tra mỗi cách cài đặt, Turing bắt đầu hình dung ra ba máy riêng biệt, mỗi máy thực hiện việc mã hóa một phần tử của vòng. Máy thứ nhất thử mã hóa **w** thành **E**, máy thứ hai thử mã hóa **e** thành **T**, và máy thứ ba mã hóa **t** thành **W**. Cả ba máy đều có cách cài đặt như nhau, ngoại trừ máy thứ hai có định hướng của các đĩa mã hóa dịch đi một vị trí so với máy đầu tiên, mà ở trên chúng ta đã gọi là S+1, và máy thứ ba có định hướng của các đĩa mã hóa dịch đi ba vị trí so với máy thứ nhất, mà chúng ta gọi là S+3. Sau đó, Turing đã hình dung một nhà giải mã điên cuồng, liên tục thay đổi các dây trong bảng ổ nối, hoán đổi các cách sắp đặt của các đĩa mã hóa và thay đổi định hướng của chúng để có được sự mã hóa đúng. Bất cứ các dây nối được thay đổi như thế nào ở máy thứ nhất thì cũng thay đổi như thế trong hai máy còn lại. Bất cứ sự sắp xếp các đĩa mã hóa thay đổi như thế nào ở máy

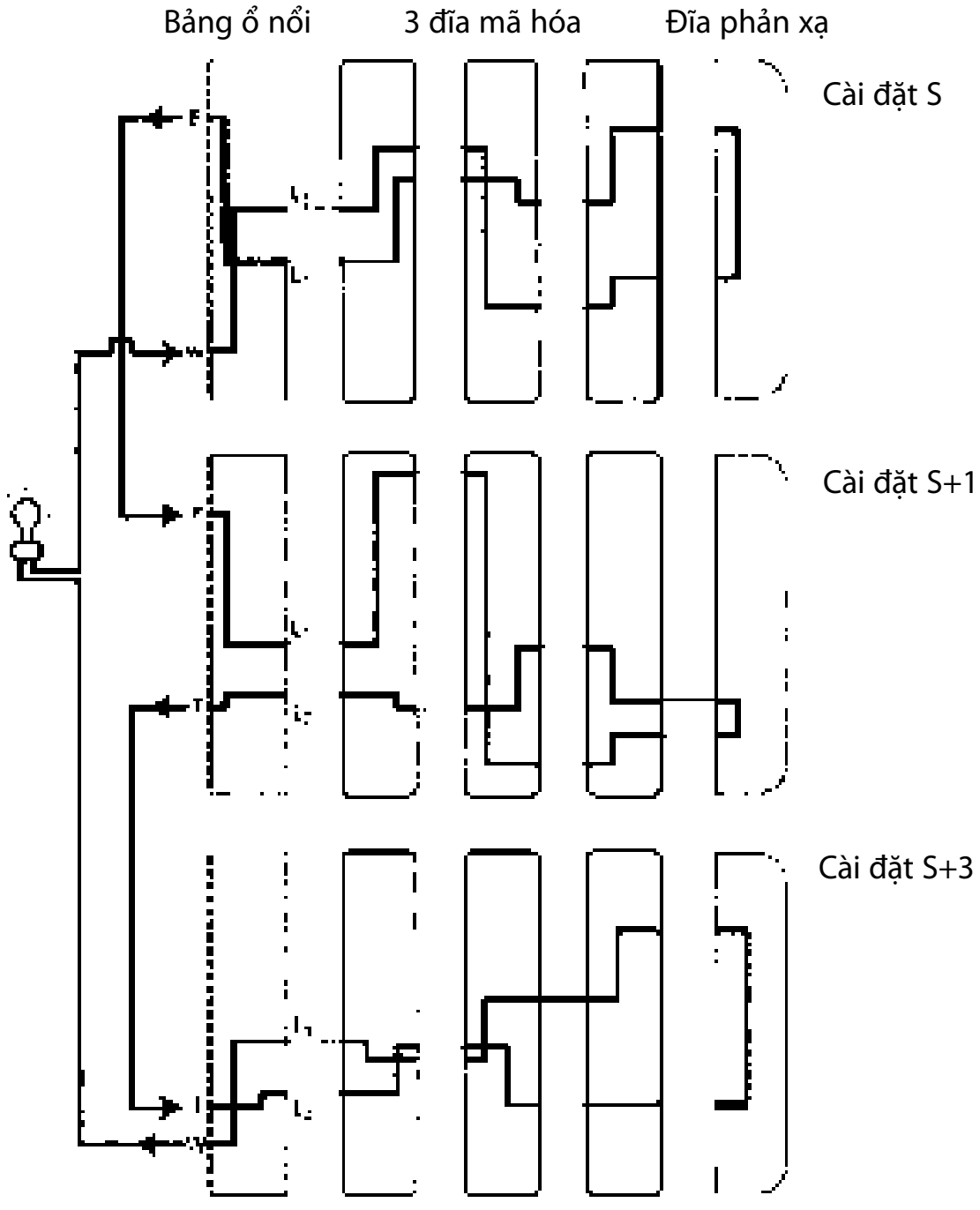


Hình 48. Một trong các *crib* của Turing, có chứa một vòng

thứ nhất thì cũng thay đổi như thế ở hai máy còn lại. Và, điều quan trọng là, bất cứ sự định hướng của các đĩa mã hóa được cài đặt như thế nào ở máy thứ nhất thì máy thứ hai cũng như thế nhưng dịch đi một vị trí, và máy thứ ba dịch đi ba vị trí.

Dường như Turing không thu được gì nhiều. Nhà giải mã vẫn phải kiểm tra tất cả 159.000.000.000.000.000.000 cách cài đặt tiềm năng, và, vấn đề còn tồi tệ hơn nữa là, giờ ông phải làm việc đồng thời với ba máy thay vì chỉ một. Tuy nhiên, giai đoạn tiếp theo trong ý tưởng của Turing đã biến đổi hoàn toàn thách thức, làm cho nó đơn giản đi rất nhiều. Ông đã nghĩ đến việc nối ba máy với nhau bằng việc chạy các dây điện giữa đầu vào và đầu ra của mỗi máy, như trên Hình 49. Kết quả là vòng trong *crib* mắc song song với vòng của dòng điện. Turing đã hình dung các máy thay đổi cài đặt bảng ổ nối và các đĩa mã hóa, như mô tả ở trên, nhưng chỉ khi tất cả các cài đặt là đúng ở tất cả ba máy thì dòng điện mới xuất hiện, cho phép dòng điện chạy qua tất cả ba máy. Nếu Turing lắp thêm vào mạch một bóng đèn thì dòng điện sẽ làm bóng đèn sáng, báo hiệu các cài đặt đúng đã được tìm thấy. Lúc này, cả ba máy vẫn phải kiểm tra 159.000.000.000.000.000.000 khả năng cài đặt để làm sáng bóng đèn. Tuy nhiên, tất cả những gì đã làm cho tới đây chỉ là một bước chuẩn bị cho sự nhảy vọt logic cuối cùng của Turing, và điều này sẽ làm cho nhiệm vụ đơn giản đi hàng trăm triệu triệu lần trong một cuộc đột kích quyết liệt.

Turing đã tạo mạch điện theo cách làm vô hiệu hóa ảnh hưởng của bảng ổ nối, nhờ đó cho phép ông bỏ qua hàng tỉ cách cài đặt trong bảng ổ nối. Hình 49 cho thấy máy Enigma đầu tiên có dòng điện đi vào qua các đĩa mã hóa và đi ra ở các chữ cái chưa biết, mà chúng ta gọi là **L1**. Dòng điện sau đó chạy qua bảng ổ



Hình 49 Vòng trong *crib* có thể được mắc song song với một vòng dòng điện. Ba máy Enigma được cài đặt giống nhau, ngoại trừ việc máy thứ hai có đĩa mã hóa thứ nhất dịch đi *một vị trí* (cài đặt S+1), và máy thứ ba có đĩa mã hóa dịch đi hai vị trí nữa (cài đặt S+3). Đầu ra của mỗi máy Enigma được nối với đầu vào của chiếc máy cạnh nó. Ba tập hợp các đĩa mã hóa phối hợp thống nhất với nhau cho đến khi mạch điện khép kín và đèn sáng. Lúc đó, cài đặt đúng đã được tìm thấy. Trong hình vẽ trên, mạch điện đã khép kín, tương ứng với cài đặt đúng.

nối, và bảng này sẽ làm biến đổi **L1** thành **E**. Chữ cái **E** này được nối với chữ cái **e** trong máy Enigma thứ hai bằng một dây dẫn, và khi dòng điện chạy qua bảng ổ nối thứ hai thì nó được chuyển đổi trở lại thành **L1**. Nói cách khác, hai bảng ổ nối tự triệt tiêu lẫn nhau. Tương tự như vậy, dòng điện chạy ra từ các đĩa mã hóa ở máy Enigma thứ hai sẽ đi vào bảng ổ nối qua **L2** trước khi bị chuyển đổi thành **T**. Chữ cái **T** này được nối qua một dây dẫn với chữ cái **t** trong máy Enigma thứ ba, và khi dòng điện chạy qua bảng ổ nối thứ ba thì nó sẽ được chuyển đổi trở lại thành **L2**. Tóm lại, các bảng ổ nối triệt tiêu lẫn nhau trong cả mạch điện, nhờ đó Turing có thể hoàn toàn bỏ qua chúng.

Turing chỉ cần nối đầu ra của tập hợp các đĩa mã hóa thứ nhất, **L1**, trực tiếp với đầu vào của tập hợp các đĩa mã hóa thứ hai, cũng là **L1** và cứ tiếp tục như vậy. Thật không may là ông không biết giá trị của **L1**, nên ông phải nối tất cả 26 đầu ra của tập hợp các đĩa mã hóa thứ nhất với 26 đầu vào tương ứng của tập hợp các đĩa mã hóa thứ hai và cứ như vậy. Kết quả là, có 26 mạch điện kín và mỗi mạch đều có một bóng điện để báo hiệu một vòng khép kín của dòng điện. Ba tập hợp các đĩa mã hóa khi đó có thể kiểm tra được 17.576 định hướng, với tập hợp thứ hai các đĩa mã hóa luôn dịch đi một bước về phía trước so với tập hợp thứ nhất và tập hợp thứ ba các đĩa mã hóa dịch đi hai bước về phía trước so với tập hợp thứ hai. Cuối cùng, khi tìm được định hướng đúng của đĩa mã hóa, một trong các mạch điện sẽ được khép kín và bóng đèn sẽ sáng. Nếu các đĩa mã hóa thay đổi định hướng trong mỗi giây thì sẽ phải mất khoảng 6 giờ để kiểm tra tất cả các định hướng.

Chỉ còn lại hai vấn đề. Thứ nhất, có thể ba máy đều chạy

với sự sắp xếp các đĩa mã hóa không đúng, vì máy Enigma vận hành với chỉ ba trong số năm đĩa mã hóa sẵn có, được đặt theo bất kỳ trật tự nào, với 60 khả năng sắp xếp khác nhau. Do đó, nếu tất cả 15.576 định hướng đã được kiểm tra, và đèn không sáng thì cần thiết phải thử một cách sắp xếp khác trong số 60 cách khả dĩ, và tiếp tục thử cho đến khi mạch điện được khép kín. Nói cách khác, các nhà giải mã cần 60 bộ ba máy Enigma chạy cùng một lúc.

Vấn đề thứ hai liên quan đến các dây nối trong bảng ổ nối, một khi sự sắp xếp các đĩa mã hóa và các định hướng đã được xác lập. Việc này thì khá đơn giản. Sử dụng một máy Enigma với sự sắp xếp các đĩa mã hóa và định hướng đĩa đúng, các nhà giải mã đánh vào văn bản mật mã và xem văn bản thường hiện ra. Nếu kết quả là **tewwer** thay vì **wetter**, thì rõ ràng là các dây trong bảng ổ nối đã nối **w** và **t** với nhau. Đánh vào các đoạn khác của văn bản mật mã sẽ phát hiện ra các hoán đổi còn lại.

Sự kết hợp giữa *crib*, các vòng và các máy nối với nhau bằng dòng điện đã mang lại kết quả đáng kể trong việc giải mã, và chỉ Turing, với vốn hiểu biết độc nhất vô nhị của mình về các máy toán học, mới có thể đạt được điều đó. Những suy ngẫm của ông về máy Turing tưởng tượng với ý định dùng để giải đáp những vấn đề gay cấn về tính không quyết định được trong toán học, song chính nghiên cứu hoàn toàn có tính chất lý thuyết này lại khiến ông nảy ra ý tưởng thiết kế một cỗ máy thực dụng có thể giải được những bài toán rất hiện thực.

Bletchley có thể kiếm được 100.000 bảng Anh để biến ý tưởng của Turing thành công cụ làm việc, cũng được mệnh danh là *bom*, vì về phương diện cơ khí nó cũng hao hao như máy *bom*

của Rejewski. Mỗi máy *bom* của Turing đều gồm có 12 tập hợp các đĩa mã hóa Enigma được nối điện với nhau, và chính vì vậy nó có thể xử lý được những vòng chữ cái dài hơn nhiều. Một máy hoàn chỉnh có thể cao đến 2 mét, dài 2 mét và rộng 1 mét. Turing hoàn tất thiết kế vào đầu năm 1940, và việc xây dựng được giao cho nhà máy British Tabulating Machinery ở Letchworth.

Trong khi chờ máy *bom* được gửi tới, Turing tiếp tục công việc hằng ngày của mình ở Bletchley. Những tin tức về đột phá của ông đã nhanh chóng lan truyền giữa những nhà giải mã cao cấp khác, và họ đều phải công nhận ông là một nhà giải mã tài năng phi thường. Theo Peter Hilton, một nhà giải mã ở Bletchley thì "Alan Turing rõ ràng là một thiên tài, song ông là một thiên tài thân thiện, dễ gần. Ông luôn luôn sẵn sàng dành thời gian và bỏ công sức để giải thích các ý tưởng của mình; song ông không phải là một chuyên gia trong một lĩnh vực hẹp, các ý tưởng phong phú của ông bao trùm một phạm vi rộng lớn của các khoa học chính xác".

Tuy nhiên, tất cả mọi thứ ở Trường Mật mã của Chính phủ đều là tối mật, nên không ai ở bên ngoài Bletchley Park biết được thành tựu to lớn của Turing. Chẳng hạn, bố mẹ ông thậm chí hoàn toàn không biết Alan là một nhà giải mã chứ đừng nói gì đến chuyện ông là một nhà giải mã hàng đầu của nước Anh. Ông đã từng nói với mẹ mình rằng ông có tham gia vào một số nghiên cứu về quân sự, nhưng ông không giải thích cụ thể. Bà chỉ thấy thất vọng là điều đó đã không làm cho cậu con trai lôi thôi của mình có một mái tóc trông tươm tất hơn. Mặc dù Bletchley được điều hành bởi quân đội, song họ cũng phải

nhún nhường mà chấp nhận sự lôi thôi và lập dị của các "*type* giáo sư" đó. Turing hiếm khi để tâm đến việc cạo râu, móng tay của ông thì lúc nào cũng cáu bẩn và quần áo thì luộm thuộm nhăn nhúm. Không biết quân đội có chấp nhận cả bệnh đồng tính của ông hay không thì hiện thời vẫn còn chưa được biết. Jack Good, một cựu quân nhân ở Bletchley, nhận xét "Rất may là những người có thẩm quyền đã không biết rằng Turing là một người đồng tính. Nếu không có thể chúng ta đã thua trong cuộc chiến tranh".

Máy *bom* mẫu đầu tiên, có tên *Victory,* đã đến Bletchley vào ngày 14 tháng Ba năm 1940. Máy đã được vận hành ngay lập tức, song kết quả đầu tiên không được thỏa mãn cho lắm. Máy cho kết quả chậm hơn nhiều so với dự kiến, phải mất cả tuần mới tìm ra một chìa khóa mã. Một sự nỗ lực phối hợp đã được thực thi để làm tăng hiệu quả của *bom*, và mẫu thiết kế sửa đổi đã được hoàn thành vài tuần sau đó. Phải mất thêm khoảng bốn tháng nữa để chế tạo máy *bom* đã được nâng cấp. Cùng lúc đó, các nhà giải mã lại phải đối mặt với một tai họa mà họ đã dự đoán trước. Ngày 1 tháng Năm năm 1940, người Đức đã thay đổi phương thức trao đổi khóa mã của họ. Họ không còn lặp lại khóa mã thư nữa và vì vậy mà số lượng những bức thư được giải mã thành công đã giảm xuống nhanh chóng. Sự thiếu hụt thông tin kéo dài cho đến tận ngày 8 tháng Tám, khi máy *bom* mới được gửi đến. Máy được được đặt tên là *Agnus Dei*, hay thường gọi tắt là *Agnes*, đã hoàn toàn thỏa mãn mọi mong muốn của Turing.

Trong vòng 18 tháng, đã có 15 máy *bom* được đưa vào vận hành, khai thác các *crib*, kiểm tra các cách sắp đặt các đĩa mã hóa và tìm ra các khóa mã, mỗi máy đều kêu lách cách như hàng

triệu que đan. Nếu tất cả đều suôn sẻ, thì một máy *bom* có thể tìm ra khóa mã Enigma chỉ trong vòng một giờ. Một khi cách nối dây trong bảng ổ nối và cách sắp đặt các đĩa mã hóa (chìa khóa mã thư) đã được xác định cho một bức thư nhất định thì thật dễ dàng để tìm ra khóa mã của ngày hôm đó. Tất cả các bức thư gửi đến trong ngày đều có thể được giải mã.

Mặc dù *bom* chính là một đột phá có tính chất sống còn trong giải mã, song việc giải mã vẫn chưa trở thành một thủ tục. Vẫn còn nhiều chướng ngại phải vượt qua trước khi *bom* có thể bắt đầu tìm kiếm khóa mã. Chẳng hạn, để vận hành *bom*, trước tiên phải cần có một *crib*. Các nhà giải mã cao cấp có thể đưa *crib* cho các nhà điều khiển *bom*, song không có gì bảo đảm rằng nhà giải mã này đã đoán đúng ý nghĩa của đoạn mật mã. Và ngay cả nếu họ đã có *crib* đúng thì cũng có thể nó được đặt không đúng chỗ - nhà giải mã có thể đoán rằng bức thư được mã hóa có chứa một đoạn nhất định, song lại gắn nó với đoạn mật mã không đúng. Tuy nhiên, có một mẹo đơn giản để kiểm tra liệu một *crib* có được đặt đúng chỗ hay không.

Trong *crib* dưới đây, nhà giải mã chắc chắn rằng đoạn văn bản thường là đúng, nhưng ông ta còn chưa chắc chắn mình đã khớp nó với các chữ cái đúng trong văn bản mật mã hay không.

Bảng chữ cái thường

w e t t e r n u l l s e c h s

Bảng chữ cái mật mã

I P R E N L W K M J J S X C P L E J W Q

Một trong những đặc điểm của máy Enigma, đó là nó không thể mã hóa một chữ cái thành chính nó, đây là một kết quả của đĩa phản xạ. Chữ cái **a** không bao giờ được mã hóa thành **A**, chữ

cái **b** không bao giờ mã hóa thành **B,** v.v... Chính vì vậy *crib* cụ thể ở trên đã được ghép không đúng, vì chữ cái **e** đầu tiên của từ **wetter** lại ứng với chữ cái **E** trong đoạn mật mã. Để tìm ra sự tương ứng đúng, chúng ta chỉ cần đơn giản cho trượt đoạn văn bản thường và đoạn mật mã đối với nhau cho đến khi không còn chữ cái nào cặp với chính nó nữa. Nếu chúng ta dịch đoạn văn bản thường đi một vị trí sang bên trái thì sự khớp vẫn sai vì lúc này, chữ cái **s** đầu tiên trong từ **sechs** lại cặp với chữ cái **S** trong đoạn mật mã. Tuy nhiên, nếu chúng ta dịch đi một vị trí sang bên phải thì không có sự vi phạm nào. Vì vậy, *crib* đã chắc chắn là ở đúng vị trí, và đã có thể được sử dụng làm cơ sở để giải mã bằng *bom*.

Bảng chữ cái thường

w e t t e r n u l l s e c h s

Bảng chữ cái mật mã

I P R E N L W K M J J S X C P L E J W Q

Tin tức tình báo thu thập được ở Bletchley chỉ được chuyển cho những nhân vật quân sự cấp cao nhất và những thành viên được lựa chọn từ nội các chiến tranh. Winston Churchill đã ý thức được một cách đầy đủ về tầm quan trọng của việc giải mã ở Bletchley và vào ngày 6 tháng Chín năm 1941, ông đã đến thăm các nhà giải mã. Trong cuộc gặp với một số nhà giải mã, ông đã rất ngạc nhiên trước một tập hợp kỳ quặc những người đã cung cấp cho ông những thông tin có giá trị đến như vậy; ngoài các nhà toán học và ngôn ngữ học, còn có một chuyên gia về gốm, một người phụ trách về bảo tàng đến từ Bảo tàng Praha, một kiện tướng cờ vua người Anh và rất nhiều các chuyên gia về bài bridge. Churchill đã thì thầm với Ngài Stewart Menzies, người

đứng đầu Cơ quan Tình báo Anh: "Tôi đã yêu cầu ông phải dùng mọi phương cách, nhưng tôi thật không ngờ là ông lại tuân lệnh tôi một cách giáo điều như vậy". Tuy nhận xét như thế, song ông vẫn rất thích thú với nhóm người này và gọi họ là "những con ngỗng đẻ trứng vàng và không bao giờ kêu quạc quạc".

Chuyến viếng thăm này là nhằm khích lệ tinh thần của các nhà giải mã bằng việc chứng tỏ cho họ thấy công việc của họ được coi trọng ở cấp cao nhất. Điều này cũng đã mang lại cho Turing và các đồng nghiệp của ông sự tự tin để có thể tiếp xúc trực tiếp với Churchill khi cuộc khủng hoảng nổ ra. Để tận dụng các máy *bom*, Turing cần thêm nhiều nhân viên, song yêu cầu của ông đã bị viên chỉ huy Edward Travis, người mới được bổ nhiệm làm Giám đốc của Bletchley, chặn lại vì y cảm thấy không có lý do gì phải tuyển thêm người nữa. Vào ngày 21 tháng Mười năm 1941, các nhà giải mã không chịu phục tùng đã lờ Travis đi và viết thư thẳng cho Churchill.

Thưa ngài Thủ tướng,

Vài tuần trước Ngài đã cho chúng tôi hân hạnh được đón Ngài tới thăm và chúng tôi tin rằng Ngài coi trọng công việc của chúng tôi. Như Ngài đã biết, phần lớn nhờ vào năng lực và tầm nhìn xa của ngài chỉ huy Travis mà chúng tôi đã được cung cấp đầy đủ các máy bom để giải mật mã Enigma của người Đức. Tuy nhiên, chúng tôi cho rằng Ngài cũng nên biết là công việc này cần phải được ủng hộ và trong một số trường hợp đã không được hoàn thành, cơ bản là vì chúng tôi không có đủ số lượng nhân viên cần thiết để làm việc. Lý do chúng tôi viết thư trực tiếp cho Ngài là vì trong nhiều tháng, chúng tôi đã làm đủ mọi thủ tục theo các kênh thông thường, nhưng chúng tôi đã hết

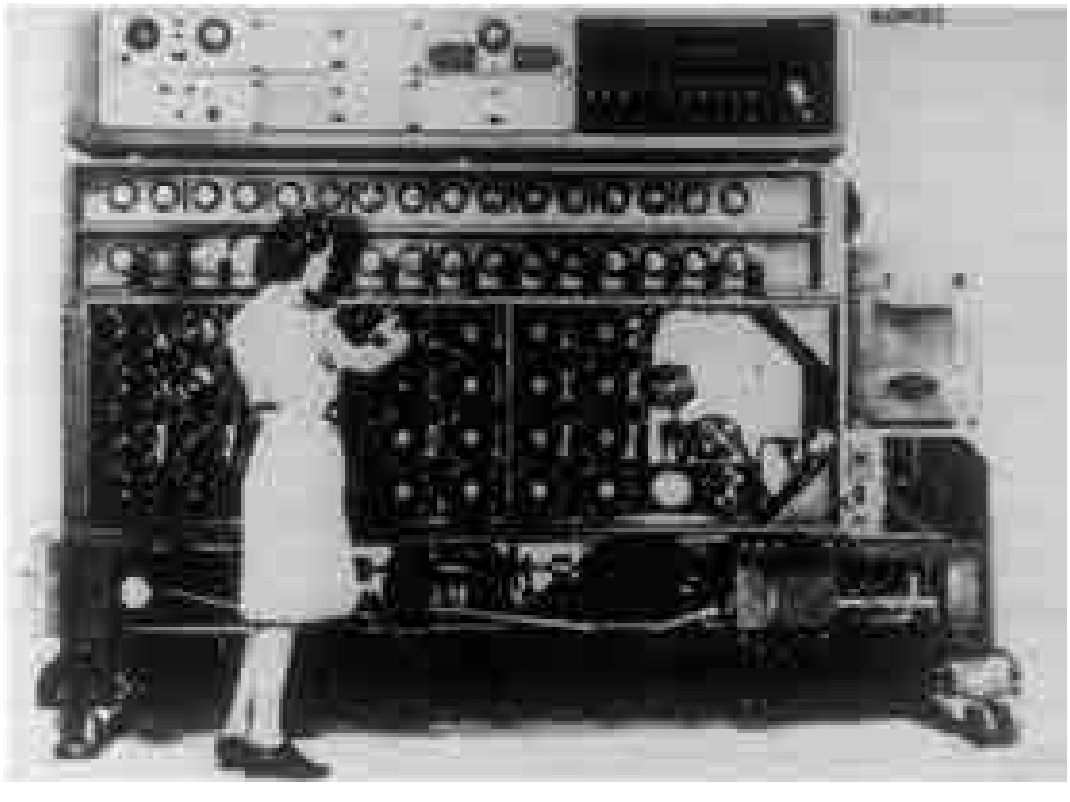
hy vọng sớm có bất kỳ sự cải thiện nào nếu không có sự can thiệp của Ngài...

Những kẻ tôi tớ tận tụy của Ngài,
A.M. Turing
W.G. Welchman
C.H.O'D. Alexander
P.S Milner Barry

Churchill đã không do dự đáp lại họ. Ông ngay lập tức đã cho viết một bản ghi nhớ cho viên chánh văn phòng của mình:

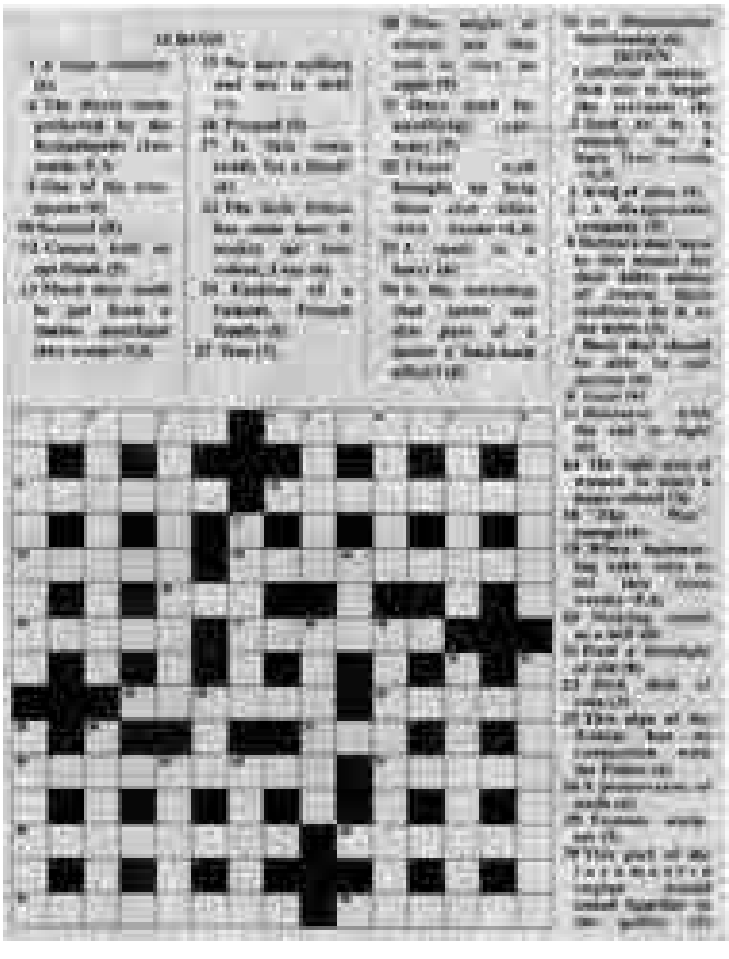
THỰC HIỆN NGAY TRONG HÔM NAY

Hãy đảm bảo rằng họ sẽ có tất cả những gì họ muốn với sự ưu tiên tối đa và báo cáo lại tôi khi việc này hoàn thành.



Hình 50 Một máy *bom* đang hoạt động

Nhờ vậy mà không còn rào cản nào nữa đối với việc tuyển thêm người hay mua thêm vật tư. Cho đến cuối năm 1942, đã có 49 máy *bom* và một trạm *bom* mới đã được khai trương ở Gayhurst Manor, ngay phía bắc của Bletchley. Như là một phần của công việc tuyển mộ, Trường Mật mã của Chính phủ đã cho đăng một bức thư trên tờ *Daily Telegraph*. Họ đã đưa ra một thử thách nặc danh cho người đọc, yêu cầu bất kỳ ai có thể giải được ô chữ của tờ báo (Hình 51) trong vòng 12 phút. Người ta cho rằng những chuyên gia về ô chữ cũng có thể là một nhà giải mã tốt, bổ sung vào những bộ não khoa học hiện có tại Bletchley, song tất nhiên điều này không được đề cập trên báo. Hai mươi lăm người đọc có lời giải đã được mời đến phố Fleet để thực hiện một bài kiểm tra về ô chữ. Năm người trong số họ đã hoàn thành ô chữ trong thời gian quy định và một người chỉ còn lại một từ khi 12 phút đã trôi qua. Một tuần sau, cả sáu người đã được cơ quan tình báo quân sự phỏng vấn và được tuyển mộ làm nhà giải mã tại Bletchley Park.



Hình 51. Ô chữ trên tờ *Daily Telegraph* được sử dụng làm bài kiểm tra để tuyển thêm các nhà giải mã mới (phần giải đáp ở Phụ lục H).

Đánh cắp sổ mã

Đến lúc này, xa lộ Enigma được coi như là một hệ thống thông tin liên lạc khổng lồ, song trong thực tế cũng còn có một vài mạng lưới khác. Chẳng hạn, Quân đội Đức ở Bắc Phi đã có một hệ thống riêng của họ, và những người điều khiển Enigma đã có những cuốn sổ mã khác với sổ mã được sử dụng ở châu Âu. Vì vậy, nếu Bletchley đã thành công trong việc xác định khóa mã ngày của Bắc Phi thì nó có thể được sử dụng để giải mã tất cả các thư từ của người Đức gửi từ Bắc Phi ngày hôm đó, song khóa mã ngày của Bắc Phi lại không sử dụng được để giải mã những thư từ gửi đi từ châu Âu.Tương tự, Luftwaffe (Không quân) cũng có hệ thống liên lạc riêng, và vì vậy để giải mã được tất cả tin tức của Luftwaffe, Bletchley sẽ phải tìm ra khóa mã ngày của Luftwaffe.

Một số hệ thống khó giải mã hơn hệ thống khác. Hệ thống Kriegsmarine là khó nhất trong tất cả, vì Hải quân Đức có được hệ máy Enigma phức tạp hơn. Chẳng hạn, người điều khiển Enigma Hải quân được lựa chọn trong tám đĩa mã hóa chứ không phải năm, điều đó có nghĩa là số cách sắp xếp các đĩa mã hóa nhiều hơn gấp sáu lần và do vậy số khóa mã mà Bletchley phải kiểm tra cũng nhiều hơn sáu lần. Sự khác biệt nữa ở Enigma Hải quân có liên quan đến đĩa phản xạ, nó có tác dụng chuyển trở lại tín hiệu điện qua các đĩa mã hóa. Ở các máy Enigma tiêu chuẩn thì đĩa phản xạ luôn cố định ở một định hướng cụ thể, nhưng trong Enigma Hải quân thì đĩa phản xạ được đặt ở một trong 26 định hướng. Như vậy, số khóa mã tiềm năng sẽ còn tăng lên 26 lần.

Việc giải mã Enigma Hải quân còn bị làm cho khó khăn hơn bởi những người điều khiển máy Hải quân, những người này rất

thận trọng để không gửi các bức thư được viết theo khuôn mẫu, do vậy không còn các *crib* cho những người ở Bletchley. Hơn thế nữa, Kriegsmarine còn sử dụng một hệ thống an toàn hơn để lựa chọn và truyền đi các khóa mã thư. Bổ sung thêm đĩa mã hóa, đĩa phản xạ thay đổi, các bức thư không viết theo khuôn mẫu và một hệ thống trao đổi khóa mã thư mới, tất cả đã góp phần làm cho thông tin liên lạc của Hải quân Đức là không thể thâm nhập nổi.

Sự thất bại của Bletchley trong việc phá vỡ Enigma Hải quân đồng nghĩa với việc Kriegsmarine dần giành lại được ưu thế trong Trận chiến Đại Tây dương. Đô đốc Karl Dônitz đã phát triển một chiến lược hai bước có hiệu quả cao cho cuộc chiến trên biển, bắt đầu bằng việc cho các tàu ngầm Đức *(U-boat)* rải ở mọi nơi và lùng sục khắp các vùng biển Đại Tây dương để săn tìm các đội tàu của quân Đồng minh. Ngay sau khi một tàu ngầm dò được mục tiêu, nó sẽ bắt đầu bước tiếp theo của chiến lược là gọi các tàu ngầm khác đến hiện trường. Cuộc tấn công chỉ bắt đầu khi một số lượng lớn tàu ngầm đã được tập hợp. Để cho chiến lược tấn công tổng lực này được thành công, điều quan trọng là Kriegsmarine phải có được một hệ thống liên lạc an toàn. Enigma Hải quân đã cung cấp một hệ thống như vậy và cuộc tấn công tàu ngầm đã có một ảnh hưởng khủng khiếp đến việc vận chuyển bằng đường thủy của quân Đồng minh bởi nó cung cấp một lượng lớn nhu yếu phẩm và vũ khí cho nước Anh.

Chừng nào mà liên lạc giữa các tàu ngầm Đức còn an toàn, thì quân Đồng minh sẽ không biết được vị trí của các tàu ngầm Đức và không thể tìm ra con đường an toàn cho các đội tàu. Dường như chiến lược duy nhất của Bộ Hải quân để tìm ra vị trí của các tàu ngầm Đức, đó là nhìn vào những nơi có các tàu Anh bị đánh

đắm. Trong vòng từ tháng Sáu năm 1940 đến tháng Sáu năm 1941, quân Đồng minh đã bị mất trung bình khoảng 50 tàu mỗi tháng và họ lâm vào tình trạng nguy kịch vì không thể đóng tàu mới kịp để thay thế. Bên cạnh việc số lượng tàu giảm đi quá nhanh, còn có một sự mất mát khủng khiếp về con người - 50.000 thủy thủ quân Đồng minh đã chết trong chiến tranh. Nếu những mất mát này không giảm đi nhanh chóng thì người Anh sẽ có nguy cơ thất bại trong Trận chiến Đại Tây dương, và như thế có nghĩa là thất bại trong cả cuộc chiến tranh. Churchill sau này đã viết, "Giữa dòng chảy của những sự kiện dữ dội, một sự lo ngại bao trùm đến tột cùng. Những cuộc chiến có thể thắng hoặc thua, các kế hoạch có thể thành công hoặc thất bại, lãnh thổ có thể chiếm lại hoặc bị mất, song vượt lên trên tất cả sức mạnh mà chúng tôi mang theo trong cuộc chiến tranh, hay thậm chí giữ lại mạng sống của mình, đó là phải kiểm soát đường biển và tự do ra vào các bến cảng".

Kinh nghiệm của người Ba Lan và trường hợp Hans-Thilo Schmidt đã dạy cho Bletchley Park một bài học là nếu những nỗ lực về trí tuệ thất bại trong việc giải mã thì cần thiết phải dựa vào hoạt động gián điệp, xâm nhập và đánh cắp để có được khóa mã của kẻ thù. Một cách ngẫu nhiên, Bletchley đã có được một thành công trước Enigma Hải quân nhờ một thủ đoạn rất thông minh của RAF *(Không quân Hoàng gia* - ND). Máy bay của Anh sẽ rải mìn ở một số vị trí nhất định, lừa cho các tàu thủy Đức gửi tin cảnh báo cho các đội tàu khác. Những tin cảnh báo được mã hóa bằng Enigma này chắc chắn có ghi chú bản đồ, song điều quan trọng là những ghi chú bản đồ này phía Anh đã biết nên nó có thể được sử dụng như là một *crib*. Nói cách khác, Bletchley

biết rằng trong văn bản mật mã nhất định sẽ phải có một đoạn cụ thể nào đó chỉ tọa độ. Việc rải mìn để có *crib* được gọi lóng là "làm vườn", đòi hỏi RAF phải bay những chuyến bay đặc biệt, nên điều này không thể làm một cách đều đặn được. Bletchley phải tìm một cách khác để hóa giải Enigma Hải quân.

Một chiến lược khác nhằm phá vỡ Enigma Hải quân dựa trên việc đánh cắp khóa mã. Một trong những kế hoạch táo bạo nhất để làm việc này do Ian Fleming, người đã sáng tạo ra nhân vật James Bond và là một thành viên của Tình báo Hải quân trong chiến tranh, nghĩ ra. Ông đề nghị cho rơi một chiếc máy bay ném bom của Đức bị bắt xuống eo biển Măngsơ, gần tàu của quân Đức. Các thủy thủ Đức sẽ tiến lại gần máy bay để cứu đồng đội của mình, nhưng phi hành đoàn ở đó là những phi công Anh giả làm người Đức, sẽ nhảy lên tàu và chiếm lấy sổ mã. Những sổ mã này của Đức có chứa các thông tin cần thiết cho việc thiết lập khóa mã và vì các tàu thường ở rất xa bờ trong một thời gian dài nên các sổ mã cũng thường có giá trị ít nhất là một tháng. Bằng cách lấy các sổ mã như vậy, Bletchley có thể giải được mã Enigma của Hải quân trong một tháng.

Sau khi thông qua kế hoạch của Fleming, được gọi tên là Chiến dịch Tàn nhẫn, Tình báo Anh bắt đầu chuẩn bị một máy bay ném bom Heinkel cho cú hạ cánh khẩn cấp, và tập hợp một phi hành đoàn người Anh nói được tiếng Đức. Kế hoạch dự định tiến hành vào đầu tháng để có thể bắt được sổ mã mới. Fleming đã đi đến Dover để chứng kiến chiến dịch, song không may là không có tàu Đức nào ở khu vực này nên kế hoạch đã bị trì hoãn vô thời hạn. Bốn ngày sau, Frank Birch, người đứng đầu bộ phận Hải quân ở Bletchley, đã kể lại phản ứng của Turing và đồng nghiệp

của ông là Peter Twinn như sau: "Turing và Twinn đã đến chỗ tôi như những người chuyên lo việc mai táng bị lừa mất một thi thể hai ngày trước đây, cả hai đều tức giận về chuyện hủy bỏ Chiến dịch Tàn nhẫn".

Mặc dù Chiến dịch Tàn nhẫn bị hủy bỏ song sổ mã Hải quân Đức cuối cùng cũng vẫn lấy được nhờ một loạt những cuộc đột kích táo bạo vào các tàu dự báo thời tiết và tàu ngầm của Đức. Cái được gọi là "sự đánh cắp" đã mang về cho Bletchley những tài liệu cần thiết để chấm dứt sự thiếu hụt tin tức tình báo. Với việc Enigma Hải quân đã trở nên "trong suốt", Bletchley đã có thể xác định được vị trí của các tàu ngầm và Trận chiến Đại Tây dương đã bắt đầu nghiêng ưu thế về phía quân Đồng minh. Các đội tàu đã có thể tránh xa các tàu ngầm Đức và thậm chí các tàu tiêu diệt của Anh đã bắt đầu phản công, săn lùng và đánh đắm tàu ngầm Đức.

Vấn đề sống còn là làm sao để Tổng hành dinh cấp cao Đức không bao giờ được nghi ngờ rằng quân Đồng minh đã đánh cắp được sổ mã. Nếu người Đức phát hiện sự an toàn của họ đã bị phá vỡ thì họ sẽ nâng cấp các máy Enigma, và Bletchley sẽ lại trở về điểm số không. Như với câu chuyện về bức điện tín Zimmermann, người Anh đã rất thận trọng để tránh gây nghi ngờ, chẳng hạn như đánh đắm tàu Đức sau khi đã đánh cắp sổ mã. Điều này sẽ thuyết phục được Đô đốc Dônitz rằng các tư liệu về mật mã đã chìm xuống đáy biển và không rơi vào tay quân Anh.

Một khi sổ mã đã được chiếm một cách bí mật thì việc sử dụng các tin tức tình báo thu được cũng phải được thực hiện thận trọng hơn. Chẳng hạn, việc giải mã Enigma cho biết rất nhiều vị trí của tàu ngầm, song sẽ thật không thông minh nếu tấn công tất cả các tàu ngầm đó, vì một sự thành công tăng lên bất ngờ

không lý giải nổi của quân Anh sẽ báo động cho quân Đức rằng các thông tin của họ đã bị giải mã. Chính vì vậy, quân Đồng minh đã cho phép một số tàu ngầm chạy thoát và tấn công những tàu ngầm khác, chỉ khi một máy bay thám thính đã được lệnh bay tới đó trước, nhờ đó mà biện minh được cho sự tiến đến của các tàu tiêu diệt sau đó vài giờ. Hoặc một lựa chọn khác, quân Đồng minh gửi các bức thư giả mô tả việc nhìn thấy các tàu ngầm Đức nhằm hợp lý hóa cho các cuộc tấn công sau đó.

Mặc dù đã có chính sách giảm thiểu tối đa những dấu hiệu để lộ ra rằng Enigma đã bị phá vỡ, song hành động của quân Anh đôi khi cũng gây sự lo ngại giữa các chuyên gia an ninh của Đức. Một lần, Bletchley giải mã được một bức thư Enigma cho biết vị trí chính xác của một nhóm tàu chở dầu và tàu quân nhu của Đức, tổng cộng tất cả là chín chiếc. Bộ Hải quân quyết định sẽ không đánh đắm tất cả các tàu vì sự quét sạch mục tiêu sẽ khiến quân Đức nghi ngờ. Thay vì vậy, họ đã thông báo cho các tàu tiêu diệt vị trí chính xác của bảy tàu, điều này cho phép tàu *Gedania* và *Gonzenheim* chạy thoát mà không hề hấn gì. Bảy tàu mục tiêu đã bị đánh đắm, nhưng Hải quân Hoàng gia đã vô tình bắt gặp hai tàu kia, mà lẽ ra phải được chạy thoát, và cũng đánh đắm chúng luôn. Các tàu tiêu diệt hoàn toàn không biết gì về Enigma cũng như chủ trương không gây nghi ngờ - họ chỉ tin rằng mình đã làm đúng phận sự của mình. Trở về Berlin, Đô đốc Kurt Fricke đã mở cuộc điều tra về việc này và các cuộc tấn công tương tự, kiểm tra khả năng có thể quân Anh đã hóa giải được Enigma. Báo cáo kết luận rằng nhiều tổn thất to lớn này hoặc là do sự không may tự nhiên, hoặc do điệp viên Anh đã xâm nhập vào Kriegsmarine. Sự giải mã Enigma được coi là không thể và không tưởng tượng được.

Các nhà giải mã vô danh

Cùng với việc hóa giải mật mã Enigma của Đức, Bletchley Park cũng thành công trong việc giải mã các thông tin của Nhật Bản và Italia. Các thông tin tình báo thu nhận được từ ba nguồn này được đặt mật danh là Ultra, và các hồ sơ Tình báo Ultra có trách nhiệm giúp cho quân Đồng minh có được một lợi thế rõ ràng trên tất cả các vũ đài trọng yếu của cuộc chiến. Ở Bắc Phi, Ultra đã hỗ trợ cho việc tiêu diệt các đường tiếp tế của Đức và thông báo cho quân Đồng minh về tình trạng lực lượng của Tướng Rommel, giúp cho Quân đoàn 8 đánh bại đội quân tiên phong của Đức. Ultra cũng đã cảnh báo về sự xâm lược của Đức vào Hy Lạp, giúp cho đội quân Anh ứng phó kịp, nên không bị thiệt hại nặng nề. Trong thực tế, Ultra đã cung cấp những báo cáo chính xác về tình hình của kẻ thù trên toàn vùng Địa Trung hải. Những thông tin này lại càng đặc biệt có giá trị khi mà quân Đồng minh đổ bộ vào Italia và Sicily năm 1943.

Năm 1944, Ultra đã đóng một vai trò chủ yếu trong cuộc đổ bộ của quân Đồng minh vào châu Âu. Chẳng hạn, trong vài tháng trước ngày D (ngày quân Anh-Mỹ đổ bộ lên miền Bắc nước Pháp), việc giải mã của Bletchley đã cung cấp một bức tranh chi tiết về sự tập trung quân của Đức dọc bờ biển nước Pháp. Ngài Harry Hinsley, nhà lịch sử quân sự của Tình báo Anh trong thời kỳ chiến tranh, đã viết:

> Khi (thông tin tình báo) Ultra được gia tăng, nó đã gây ra một vài cú sốc không mấy dễ chịu. Đặc biệt là nó đã tiết lộ vào nửa cuối tháng Năm - tiếp sau những dấu hiệu đáng lo ngại ban đầu cho thấy người Đức đã quyết định rằng vùng lãnh thổ nằm

giữa Le Havre và Cherbourg chắc chắn sẽ là vùng tấn công, và thậm chí có thể là vùng tấn công chủ yếu - rằng họ (quân Đức) đang gửi thêm quân tiếp viện tới Normandy và vùng bán đảo Cherbourg. Song chứng cứ này đã đến đúng lúc, giúp quân Đồng minh có thể điều chỉnh kế hoạch đổ bộ vào bãi biển Utah; và có một thực tế đặc biệt là trước khi cuộc viễn chinh khởi hành, ước tính của quân Đồng minh về số lượng, nhận dạng và vị trí các sư đoàn địch ở miền tây, tổng cộng gồm năm mươi tám, là chính xác về tổng số, nhưng có hai điều là quan trọng về phương diện tác chiến.

Trong suốt cuộc chiến tranh, các nhà giải mã Bletchley đã biết rằng việc giải mã của họ có tầm quan trọng sống còn, và cuộc tới thăm của Churchill càng khẳng định thêm quan điểm này. Song các nhà giải mã không bao giờ được cho biết các chi tiết của chiến dịch hay được biết những thông tin giải mã của họ đã được sử dụng như thế nào. Chẳng hạn, các nhà giải mã không hề được cho biết thông tin nào về ngày D và họ đã lập kế hoạch tổ chức một buổi khiêu vũ vào ngay buổi tối hôm trước cuộc đổ bộ. Điều này khiến viên chỉ huy Travis, Giám đốc Bletchley và là người duy nhất ở đó biết được tin cơ mật về ngày D, lo lắng. Ông ta không thể yêu cầu Ban Khiêu vũ của Nhà số 6 hủy bỏ sự kiện này vì điều đó sẽ chẳng khác gì một gợi ý rõ ràng rằng một cuộc tấn công lớn đang tới gần và như vậy là vi phạm quy tắc an ninh. Buổi khiêu vũ vẫn được phép tiến hành. Tình cờ, do thời tiết xấu, nên cuộc đổ bộ đã bị hoãn lại 24 giờ, nhờ đó mà các nhà giải mã đã có đủ thời gian để lại sức sau cuộc vui thâu đêm. Vào ngày đổ bộ, quân kháng chiến Pháp đã phá hủy phương tiện viễn thông trên đất liền, buộc quân Đức phải liên

lạc bằng vô tuyến, điều này đã giúp cho Bletchley có cơ hội để chặn bắt và giải mã thêm nhiều thông tin hơn. Vào thời điểm có tính bước ngoặt này của cuộc chiến, Bletchley đã có thể cung cấp một bức tranh còn chi tiết hơn nữa về các chiến dịch quân sự của Đức.

Stuart Milner-Barry, một trong số các nhà giải mã của Nhà số 6 đã viết: "Tôi không thể tưởng tượng được là có cuộc chiến tranh nào từ thời xưa lại diễn ra mà trong đó một phía đọc được đều đặn các tin tình báo hải quân và lục quân của phía bên kia". Một báo cáo của Mỹ cũng có kết luận tương tự: "Ultra đã tạo ra trong các bộ tham mưu cao cấp và tại thời điểm cao trào về chính trị, một trạng thái tinh thần có thể làm thay đổi việc ra quyết định. Cảm giác đi guốc vào bụng kẻ thù thật là một cảm giác vô cùng thoải mái. Nó tăng dần theo thời gian một cách khó có thể cảm nhận được khi bạn quan sát một cách đều đặn và đầy đủ những suy nghĩ, cách thức, thói quen và hành động của đối phương. Biết như vậy sẽ khiến kế hoạch của bạn ít do dự hơn và chắc chắn hơn, ít đau khổ hơn và vui vẻ hơn."

Mặc dù còn gây tranh cãi, nhưng người ta vẫn nhất trí cho rằng, những thành tựu của Bletchley là nhân tố quyết định trong chiến thắng của quân Đồng minh. Chí ít thì các nhà giải mã ở Bletchley đã làm rút ngắn đáng kể cuộc chiến tranh. Điều này sẽ trở nên rõ ràng nếu ta quay trở lại Trận chiến Đại Tây dương và thử tưởng tượng xem điều gì sẽ xảy ra nếu không có những tin tức tình báo Ultra. Bắt đầu là việc nhiều tàu và quân nhu bị mất bởi sự thống trị của những hạm đội tàu ngầm Đức, điều này sẽ làm tổn hại đến mối liên kết sống còn với Mỹ và buộc quân Đồng minh phải huy động nhân lực và nguồn lực vào việc đóng mới

tàu. Các nhà lịch sử đã ước tính rằng điều này sẽ trì hoãn các kế hoạch của quân Đồng minh tới vài tháng, và điều này cũng đồng nghĩa với việc lui lại cuộc tấn công vào ngày D ít nhất là cho đến năm sau. Theo Ngài Harry Hinsley, "chiến tranh, thay vì kết thúc vào năm 1945, sẽ phải kết thúc vào năm 1948 nếu Trường Mật mã của Chính phủ không thể đọc được mật mã Enigma và cung cấp các tin tức tình báo Ultra."

Trong thời gian trì hoãn này, không thể tránh khỏi sẽ có thêm nhiều người bị thiệt mạng ở châu Âu và Hitler sẽ có thể sẽ sử dụng mạnh hơn vũ khí V, gây thêm thiệt hại trên khắp miền nam nước Anh. Nhà sử học David Kahn đã tóm tắt lại ảnh hưởng của việc giải mã Enigma như sau: "Nó đã cứu nhiều mạng sống. Không chỉ là người Nga và quân Đồng minh mà, nhờ rút ngắn cuộc chiến tranh, cả mạng sống của những người Đức, Italia và Nhật Bản. Một số người sống sót sau Thế chiến Thứ hai này có thể không phải trực tiếp nhưng cũng là nhờ có những giải mã đó. Đây là một món nợ mà cả thế giới phải mang ơn các nhà giải mã; đó là giá trị nhân bản tột bực của chiến thắng của họ".

Sau chiến tranh, thành công của Bletchley vẫn còn là một điều bí mật được bảo vệ chặt chẽ. Nhờ có những bức thư được giải mã thành công trong chiến tranh, nước Anh vẫn muốn tiếp tục các chiến dịch tình báo và do dự không muốn tiết lộ những khả năng của mình. Trong thực tế, Anh đã bắt được hàng ngàn máy Enigma và phân phối chúng cho các thuộc địa trước đây của mình, nơi vẫn tin rằng chúng là mật mã an toàn như người Đức vẫn tưởng. Người Anh không làm gì để ngừng lợi dụng lòng tin của họ và vẫn đều đặn giải mã những thông tin liên lạc mật của họ trong nhiều năm sau đó.

Trong khi đó, Trường Mật mã của Chính phủ ở Bletchley Park đã đóng cửa và hàng ngàn đàn ông và phụ nữ, những người đã góp phần tạo nên Ultra, đã bị giải tán. Các máy *bom* bị tháo dỡ và mọi giấy tờ có liên quan đến việc giải mã trong thời kỳ chiến tranh hoặc là được cất giấu hoặc bị đốt hết. Các hoạt động giải mã của Anh chính thức được chuyển sang cho Tổng hành dinh Thông tin Liên lạc của Chính phủ (GCHQ) mới được thành lập ở London và chuyển trụ sở đến Cheltenham vào năm 1952. Mặc dù một số nhà giải mã cũng chuyển sang GCHQ song hầu hết đều trở về cuộc sống dân sự. Họ phải thề giữ bí mật, không được tiết lộ về vai trò then chốt của họ trong những nỗ lực của quân Đồng minh thời chiến. Trong khi những người chiến đấu trên mặt trận bình thường khác đều có thể nói về những chiến công của mình thì những người chiến đấu trên mặt trận trí óc không hề ít quan trọng hơn lại phải chịu đựng sự lúng túng khi phải thoái thác những câu hỏi về hoạt động của họ trong chiến tranh. Gordon Welchman kể lại chuyện một trong những nhà giải mã trẻ cùng làm việc với ông ở Nhà số 6 đã nhận được một bức thư mỉa mai cay độc từ ông hiệu trưởng cũ, buộc tội ông là nỗi nhục nhã của nhà trường vì đã không dám ra mặt trận. Derek Taunt, người cũng làm việc ở Nhà số 6, đã tóm tắt lại những đóng góp thật sự của ông với đồng nghiệp: "Nhóm làm việc hạnh phúc của chúng tôi có thể đã không cùng với King Harry có mặt vào Ngày Thánh Crispin, nhưng chúng tôi chắc chắn đã không rúc trong chăn và không có lý do gì để phải tự nguyền rủa những gì đã diễn ra nơi mà chúng tôi đã ở".

Sau ba thập kỷ im lặng, bí mật về Bletchley Park cũng dần đi đến hồi kết vào đầu những năm 1970. Đại úy F.W. Winterbotham,

người chịu trách nhiệm phân phối các tin tức tình báo Ultra, bắt đầu kiến nghị với Chính phủ Anh, với lý lẽ rằng hiện các quốc gia trong Khối Thịnh vượng chung đã ngừng sử dụng mật mã Enigma và rằng lúc này cũng sẽ chẳng thiệt hại gì nếu thừa nhận thực tế rằng người Anh đã từng hóa giải được nó. Các cơ quan tình báo chấp thuận một cách e ngại, nhưng vẫn cho phép ông viết một cuốn sách về những công việc đã làm tại Bletchley Park. Được xuất bản vào mùa hè năm 1974, cuốn sách của Winterbotham có tên *Bí mật Ultra* chính là tín hiệu để các cá nhân của Bletchley cuối cùng đã được tự do lên tiếng về những hoạt động của họ trong chiến tranh. Gordon Welchman cảm thấy cực kỳ nhẹ nhõm: "Sau chiến tranh, tôi vẫn tránh nói đến những sự kiện trong chiến tranh vì sợ rằng tôi có thể tiết lộ những thông tin có được từ Ultra chứ không phải là từ sự tường thuật nào đó đã được công bố... Tôi cảm thấy bước ngoặt này đã giải phóng tôi khỏi những cam kết giữ bí mật của mình thời chiến tranh".

Những người đã đóng góp quá nhiều cho những nỗ lực trong chiến tranh giờ đã có thể nhận được sự chú ý mà họ đáng được hưởng. Có lẽ kết quả đáng kể nhất của các tiết lộ của Winterbotham đó là Rejewski đã biết được những kết quả đáng ngạc nhiên của những thành tựu chống lại Enigma trước chiến tranh của mình. Sau khi Ba Lan bị xâm chiếm, Rejewski trốn sang Pháp và khi Pháp bị chiếm đóng thì ông lại bay sang Anh. Theo lẽ tự nhiên thì lẽ ra ông phải được góp phần vào nỗ lực giải mã Enigma của Anh, nhưng thay vì thế, ông lại bị giáng xuống làm công việc giải mã tầm thường ở một đơn vị tình báo nhỏ ở Boxmoor, gần Hemel Hempstead. Không rõ tại sao một trí tuệ sáng chói như vậy lại bị loại ra khỏi Bletchley Park, nhưng

cũng chính vì vậy mà ông hoàn toàn không hay biết gì về các hoạt động của Trường Mật mã của Chính phủ. Trước khi cuốn sách của Winterbotham được xuất bản, Rejewski vẫn không biết rằng những ý tưởng của ông đã mang lại cơ sở cho việc giải mã Enigma thường xuyên trong suốt cuộc chiến tranh.

Đối với một số người thì việc xuất bản cuốn sách của Winterbotham là quá muộn. Nhiều năm sau cái chết của Alastair Denniston, giám đốc đầu tiên của Bletchley, con gái ông mới nhận được một bức thư từ một đồng nghiệp của cha mình: "Cha của cháu là một người đàn ông vĩ đại mà tất cả những người nói tiếng Anh sẽ còn phải mang ơn trong một thời gian rất dài, nếu không muốn nói là mãi mãi. Vì vậy việc rất ít người biết chính xác những gì cha cháu đã làm quả là một chuyện đáng buồn".

Alan Turing là một nhà giải mã khác đã sống không đủ lâu để nhận được bất kỳ sự thừa nhận nào của công chúng. Thay vì được tuyên dương là một anh hùng, ông lại bị phiền toái vì bệnh đồng tính của mình. Năm 1952, trong khi khai báo với cảnh sát về một vụ trộm, ông đã thật thà khai mình có quan hệ đồng tính. Cảnh sát đã thấy không còn lựa chọn nào khác là phải bắt và phạt ông với tội danh "có hành vi thô tục, rất không đứng đắn vi phạm Điều 11 của Đạo luật sửa đổi năm 1885 của Luật tội phạm". Các báo đã đưa tin về phiên xét xử và kết án sau đó, và Turing đã bị làm nhục một cách công khai.

Bí mật của Turing bị phơi bày và giới tính của ông giờ đây đã được biết đến rộng rãi. Chính phủ Anh đã rút giấy phép không cho ông được tiếp cận với các tài liệu mật và tham gia các dự án bí mật có liên quan tới sự phát triển máy tính. Ông bị buộc phải chịu tư vấn về tâm thần và điều trị hormon, việc này đã khiến

ông bị bệnh bất lực và béo phì. Suốt hai năm sau đó, ông trở nên chán nản trầm trọng và ngày 7 tháng Sáu năm 1954, ông đã lên giường với một chai dung dịch xianua và một quả táo. Hai mươi năm trước, ông đã bị ám ảnh bởi giai điệu bài hát của mụ Phù thủy Độc ác: "Nhúng quả táo vào rượu, Để cho cái chết lịm dần thấm qua". Giờ đây ông đã sẵn sàng làm theo bùa chú của mụ ta. Ông nhúng quả táo vào xianua và cắn một vài miếng. Mới chỉ ở tuổi 42, một trong những thiên tài thực sự của khoa học giải mã đã bị buộc phải tự tử.

5

Rào cản ngôn ngữ

Trong khi những nhà giải mã người Anh hóa giải được mật mã Enigma của người Đức và làm thay đổi diễn tiến của cuộc chiến tranh ở châu Âu, thì các nhà giải mã Mỹ cũng đã có sự ảnh hưởng quan trọng không kém đối với các sự kiện trên vũ đài Thái Bình dương bằng việc phá vỡ mật mã máy của người Nhật với tên gọi là *Purple* (Màu tím). Chẳng hạn, vào tháng Sáu năm 1942, người Mỹ đã giải mã được một bức thư trong đó tóm tắt một kế hoạch của người Nhật nhằm kéo lực lượng Hải quân Hoa Kỳ đến quần đảo Aleutian bằng một trận đánh giả, trong khi mục tiêu chính của họ là đảo Midway. Mặc dù, các tàu Mỹ giả vờ trúng kế và rời Midway, song họ đã không đi quá xa. Khi các nhà giải mã Mỹ chặn bắt được và giải mã mật lệnh tấn công Midway của Nhật, các tàu lập tức quay trở lại bảo vệ hòn đảo - đây là một trong những trận đánh quan trọng nhất trong toàn bộ cuộc chiến ở Thái Bình dương. Theo Đô đốc Chester Nimitz, chiến thắng của người Mỹ ở Midway "thực chất là một chiến

thắng trong lĩnh vực tình báo. Trong khi cố gắng để tạo bất ngờ thì chính người Nhật lại bị bất ngờ".

Gần một năm sau đó, các nhà giải mã Mỹ đã bắt và giải mã được bức thư trong đó chỉ rõ lịch trình cuộc viếng thăm bắc đảo Solomon của Đô đốc Isoruko Yamamoto, Tổng tư lệnh của Hạm đội Nhật Bản. Nimitz quyết định cử máy bay chiến đấu để chặn đánh máy bay của Yamamoto. Yamamoto, vốn nổi tiếng là một người cực kỳ đúng giờ, đã đến điểm hẹn đúng 8 giờ 00 sáng, như đã ghi trong lịch trình mà người Mỹ bắt được. Chờ đón gặp ông ta là mười tám máy bay chiến đấu P-38 của Mỹ. Họ đã thành công trong việc hạ sát một trong những nhân vật có ảnh hưởng nhất trong Bộ chỉ huy cấp cao của Nhật Bản.

Mặc dù Purple và Enigma, mật mã của Nhật và Đức, cuối cùng đã bị phá vỡ, song chúng đã mang lại một mức độ an toàn nhất định khi mới được tạo ra và đặt ra những thách thức thực sự cho các nhà giải mã Anh và Mỹ. Trong thực tế, nếu các mật mã này được sử dụng một cách hợp lý - không lặp lại khóa mã thư, không có *cilly*, không có sự hạn chế trong việc cài đặt bảng ổ nối và sắp xếp các đĩa mã hóa, và không có các bức thư viết theo khuôn mẫu tạo ra các *crib* - thì hoàn toàn có thể là chúng sẽ chẳng bao giờ bị phá vỡ cả.

Sức mạnh và tiềm năng thực sự của mật mã máy được minh họa bởi mật mã Typex (hay Type X) của quân đội và không lực Anh, và mật mã SIGABA (hay M-143-C) của quân đội Mỹ. Cả hai loại mật mã này đều phức tạp hơn Enigma và cả hai đều được sử dụng hợp lý, và vì vậy chúng đều không bị phá vỡ trong suốt thời kỳ chiến tranh. Các nhà tạo mã của quân Đồng minh đã tự tin rằng mật mã máy điện-cơ phức tạp có thể bảo vệ an toàn

cho thông tin liên lạc của họ. Tuy nhiên, mật mã máy phức tạp không phải là cách thức gửi thư an toàn duy nhất. Thực sự thì một trong những hình thức mã hóa an toàn nhất được sử dụng trong Thế chiến Thứ hai lại là một dạng đơn giản nhất.

Trong suốt chiến dịch Thái Bình dương, các nhà chỉ huy Mỹ bắt đầu nhận ra rằng các máy mật mã, như SIGABA, có một trở ngại cơ bản. Mặc dù máy mã hóa điện-cơ mang lại mức độ an toàn khá cao, song nó lại chậm một cách khổ sở. Bức thư được đánh vào máy từng chữ cái một, đầu ra cũng phải ghi lại từng chữ cái và văn bản mật mã hoàn thành lại phải do các điện báo viên truyền đi. Sau khi nhận được bức thư mã hóa, các điện báo viên bên nhận lại chuyển cho chuyên gia mật mã, rồi người này lại phải lựa chọn một cách thận trọng một khóa mã đúng, và đánh bản mật mã vào một máy mật mã khác để giải mã từng chữ cái một. Thời gian và không gian dành cho hoạt động tinh vi này thì không thiếu ở chỉ huy sở hay trên tàu, song mã hóa bằng máy lại hoàn toàn không thích hợp trong những điều kiện khốc liệt và cường độ cao, như trên các đảo ở Thái Bình dương. Một phóng viên chiến tranh đã mô tả những khó khăn của thông tin liên lạc trong suốt thời gian sôi động nhất của cuộc chiến: "Khi trận chiến chỉ giới hạn trong một khu vực nhỏ thì mọi thứ đều phải tiến hành dựa trên kế hoạch căn đến từng giây. Đâu có thời gian cho việc mã hóa và giải mã. Vào lúc đó thì tiếng Anh thông thường là phương sách cuối cùng - mà càng thông tục thì càng tốt". Không may cho người Mỹ là rất nhiều lính Nhật đã học ở các trường Mỹ và thông thạo tiếng Anh, kể cả các từ tục tĩu. Do vậy mà nhiều thông tin giá trị về chiến lược và chiến thuật của Mỹ đã rơi vào tay kẻ thù.

Một trong những người phản ứng đầu tiên đối với vấn đề này là Philip Johnston, một kỹ sư người Los Angeles, tuy đã quá già không thể tham gia chiến đấu nhưng vẫn muốn đóng góp cho đất nước. Vào đầu năm 1942, ông bắt đầu đề xuất một hệ thống mã hóa bắt nguồn từ những kinh nghiệm thuở nhỏ. Là con trai một nhà truyền giáo đạo Tin lành, Johnston đã lớn lên trong vùng đất tự trị của người Navajo ở Arizona và nhờ đó mà ông hoàn toàn thông thạo văn hóa Navajo. Là một trong số rất ít người bên ngoài bộ lạc có thể nói được ngôn ngữ của họ một cách trôi chảy, do vậy ông thường phải làm phiên dịch cho các cuộc thương thảo giữa người Navajo và các đại diện của Chính phủ. Công việc của ông dựa trên năng lực này đã đạt đến đỉnh điểm trong một lần đến Nhà Trắng, khi đó mới 9 tuổi, Johnston đã dịch cho hai người Navajo muốn kiến nghị Tổng thống Theodore Roosevelt phải đối xử bình đẳng hơn với cộng đồng của họ. Ý thức được đầy đủ thứ ngôn ngữ không thể vượt qua này đối với những người ngoài bộ lạc, Johnston đã bất ngờ nhận ra rằng tiếng Navajo, hay bất kỳ một thổ ngữ nào khác ở Mỹ, đều có thể là một loại mật mã thực sự không thể phá vỡ nổi. Nếu mỗi một tiểu đoàn ở Thái Bình dương sử dụng một cặp gồm hai người thuộc cùng một bộ tộc ở Mỹ làm điện báo viên thì có thể đảm bảo được sự an toàn của thông tin liên lạc.

Ông trình bày ý tưởng này với Trung tá James E. Jones, người phụ trách về thông tin khu vực ở trại Elliott, ngay phía ngoài San Diego. Chỉ cần thốt ra một tràng tiếng Navajo với viên sĩ quan đang bối rối, Johnston đã thuyết phục được ông ta rằng ý tưởng này rất đáng được quan tâm một cách nghiêm túc. Hai tuần sau, Johnston trở lại với hai người Navajo, sẵn sàng tiến hành một cuộc thử nghiệm chứng minh trước sự chứng kiến của các sĩ

quan hải quân cao cấp. Hai người Navajo được tách riêng ra, và một người được đưa cho sáu bức thư điển hình bằng tiếng Anh mà anh ta dịch ra tiếng Navajo và chuyển cho người kia bằng vô tuyến điện. Người nhận dịch bức thư trở lại bằng tiếng Anh, viết chúng ra giấy và đưa cho các sĩ quan để so sánh với các bức thư gốc. Trò chơi tiếng Navajo đã chứng minh là không có kẽ hở nào và các sĩ quan hải quân đã chấp thuận một kế hoạch thí điểm và lệnh cho việc tuyển mộ phải bắt đầu ngay lập tức.

Tuy nhiên, trước khi tuyển mộ, trung tướng Jones và Philip Johnston phải quyết định liệu có nên thực hiện thử nghiệm với người Navajo hay với một bộ lạc khác. Johnston đã sử dụng người Navajo cho lần chứng minh đầu tiên vì ông có mối quan hệ cá nhân với bộ lạc này, song không nhất thiết lấy họ làm lựa chọn lý tưởng. Tiêu chí lựa chọn quan trọng nhất chỉ là vấn đề số lượng: hải quân cần tìm một bộ lạc có thể cung cấp một số lượng lớn người biết đọc, biết viết và có thể nói thạo tiếng Anh. Sự thiếu đầu tư của chính phủ đã dẫn tới tỷ lệ người biết chữ rất thấp ở hầu hết các vùng tự trị và vì vậy sự chú ý tập trung vào bốn bộ lạc lớn: Navajo, Sioux, Chippewa và Pima-Papago.

Navajo là bộ lạc lớn nhất nhưng lại ít học nhất, trong khi người Pima-Papago có học nhất thì lại ít hơn nhiều về số lượng. Có rất ít lựa chọn giữa bốn bộ lạc này và cuối cùng thì quyết định lại dựa vào một yếu tố quan trọng khác. Theo báo cáo chính thức về ý tưởng của Johnston:

> Navajo là bộ lạc duy nhất ở Hoa Kỳ không có dính líu với các sinh viên Đức trong suốt 20 năm qua. Những người Đức này, chuyên nghiên cứu thổ âm ở các bộ lạc khác nhau dưới vỏ bọc

là các sinh viên nghệ thuật, nhân chủng học,... chắc chắn đã có được những hiểu biết tốt về thổ âm của tất cả các bộ lạc ngoại trừ Navajo. Vì lý do này, Navajo là bộ lạc duy nhất đáp ứng được độ an toàn hoàn hảo cho loại công việc mà chúng ta đang xem xét. Cũng cần lưu ý rằng tất cả các bộ lạc khác cũng như tất cả những người khác đều hoàn toàn không hiểu nổi thổ âm Navajo, ngoại trừ hai mươi tám người Mỹ đã nghiên cứu về thổ âm này. Ngôn ngữ Navajo như là một mật mã đối với kẻ thù và thích hợp tuyệt vời cho thông tin liên lạc nhanh và an toàn.

Lúc mà nước Mỹ tham gia vào Thế chiến Thứ hai thì người Navajo vẫn đang sống trong những điều kiện khắc nghiệt và bị đối xử như những người hạ đẳng. Song hội đồng bộ lạc của họ đã đóng góp cho chiến tranh và tuyên bố lòng trung thành của mình: "Không tồn tại sự tập trung các bản tính Mỹ nào thuần khiết hơn ở những Người Mỹ Đầu tiên". Những người Navajo rất hăng hái tham gia chiến đấu, nhiều người trong số họ đã nói dối số tuổi của mình hoặc nhồi nhét hàng nải chuối và uống thật nhiều nước để có đủ số cân tối thiểu yêu cầu là 55kg. Cũng như vậy, không có gì khó khăn trong việc lựa chọn những ứng viên thích hợp làm nhiệm vụ nói mật mã Navajo khi họ đã có hiểu biết. Trong suốt bốn tháng thả bom ở Trân Châu cảng, hai mươi chín người Navajo, một số chỉ 15, 16 tuổi, đã bắt đầu quá trình liên lạc tám tuần liền với Quân đoàn Hải quân.

Trước khi khóa huấn luyện bắt đầu, Quân đoàn Hải quân phải khắc phục một vấn đề đã gây phương hại cho một loại mật mã duy nhất khác cũng dựa trên một phương ngữ Mỹ. Ở miền bắc nước Pháp, trong suốt Thế chiến Thứ nhất, Đại úy E. W. Horner thuộc đại đội D, trung đoàn bộ binh 141, đã ra lệnh tuyển mộ tám

người thuộc bộ lạc Choctaw làm điện báo viên. Dĩ nhiên là không kẻ thù nào hiểu được ngôn ngữ của họ và vì vậy tiếng Choctaw đã mang lại những thông tin liên lạc an toàn. Tuy nhiên, hệ thống mã hóa này lại có sơ hở cơ bản vì ngôn ngữ Choctaw không có các thuật ngữ quân sự hiện đại tương đương. Vì vậy, một từ kỹ thuật nào đó trong một bức thư có thể được dịch thành một cụm từ Choctaw mơ hồ khiến cho người nhận có thể hiểu sai.

Vấn đề tương tự cũng sẽ nảy sinh với ngôn ngữ của người Navajo, nhưng Quân đoàn Hải quân đã có kế hoạch thiết lập một danh sách các từ Navajo để thay cho các từ tiếng Anh không thể dịch được, vì vậy mà loại bỏ được bất kỳ sự mơ hồ nào. Những người được huấn luyện đã giúp đỡ cho việc soạn bảng từ này, với xu hướng chọn những từ mô tả thế giới tự nhiên để chỉ những từ ngữ quân sự cụ thể. Chẳng hạn, tên của các loài chim được sử dụng cho máy bay, và cá sử dụng cho tàu (xem Bảng 11). Sĩ quan chỉ huy được gọi là "tù trưởng chiến tranh", trung đội thì thành "bộ lạc bùn", công sự thì thành "đào hang" và súng cối thì gọi là "súng ngồi xổm".

Mặc dù bảng từ vựng hoàn chỉnh gồm 274 từ, song vẫn còn vấn đề trong việc dịch một số từ ít dự đoán được hơn cũng như tên người hoặc địa danh. Giải pháp là tạo ra một bảng chữ cái ngữ âm được mã hóa để đánh vần những từ khó. Chẳng hạn, từ "Pacific" (Đại Tây dương), sẽ được đánh vần là "pig, ant, cat, ice, fox, ice, cat" (lợn, kiến, mèo, băng, cáo, băng, mèo) và sau đó sẽ được dịch sang tiếng Navajo là **bi-sodih, wol-la-chee, moasi, tkin, ma-e, tkin, moasi**. Bảng chữ cái Navajo hoàn chỉnh được trình bày ở Bảng 12. Trong vòng tám tuần, các học viên nói mật mã đã học thuộc toàn bộ bảng từ vựng và bảng chữ cái, điều này

đã tránh được việc phải cần đến các cuốn sổ mã dễ bị rơi vào tay kẻ thù. Đối với người Navajo, việc ghi vào bộ nhớ tất cả mọi thứ là chuyện bình thường vì ngôn ngữ của họ về truyền thống không có chữ viết. Như William McCabe, một trong những học viên, đã nói: "ở người Navajo, mọi thứ đều ở trong bộ nhớ - các bài hát, lời cầu nguyện, tất cả. Đó là cách mà chúng tôi lớn lên."

Bảng 11. Các từ mật mã Navajo biểu thị máy bay và tàu thủy

Máy bay chiến đấu	Chim ruồi	**Da-he-tih-hi**
Máy bay do thám	Cú	**Ne-as-jah**
Máy bay thả ngư lôi	Chim én	**Tas-chizzie**
Máy bay thả bom	Chim ó	**Jay-sho**
Máy bay thả bom bổ nhào	Diều hâu	**Gini**
Bom	Trứng	**A-ye-shi**
Phương tiện thủy quân lục chiến	ếch	**Chal**
Tàu chiến	Cá voi	**Lo-tso**
Tàu khu trục	Cá mập	**Ca-lo**
Tàu ngầm	Cá sắt	**Besh-lo**

Vào cuối khóa huấn luyện, những người Navajo phải làm một bài thi. Những người gửi thì dịch một loạt thư từ tiếng Anh ra tiếng Navajo, truyền chúng đi và sau đó những người nhận thì dịch trở lại tiếng Anh, sử dụng bảng từ vựng và bảng chữ cái đã được ghi nhớ khi cần thiết. Kết quả thật hoàn hảo. Để kiểm tra sức mạnh của hệ thống, một bản ghi âm các lần truyền đã được gửi đến cho Cục tình báo Hải quân, đơn vị đã hóa giải được Purple, mật mã khó nhất của Nhật Bản. Sau ba tuần giải mã cường độ cao, các nhà giải mã Hải quân vẫn bó tay trước những bản mật mã. Họ gọi ngôn ngữ Navajo là một "tràng kỳ lạ những âm thanh khàn, giọng mũi và vặn vẹo lưỡi... chúng tôi thậm chí không thể ghi lại chứ đừng nói gì đến chuyện giải mã nó". Mật

mã Navajo đã thành công. Hai chiến binh Navajo, John Benally và Johnny Manuelito, đã được giữ lại để huấn luyện những nhóm tuyển mộ tiếp theo, trong khi hai mươi bảy người khác đã được phân về bốn trung đoàn và gửi ra mặt trận Thái Bình dương.

Bảng 12. Mã bảng chữ cái theo tiếng Navajo

A	Kiến	**Wol-la-chee**	**N**	Hạt	**Nesh-chee**
B	Gấu	**Shush**	**O**	Cú	**Ne-ahs-jsh**
C	Mèo	**Moasi**	**P**	Lợn	**Bi-sodih**
D	Hươu	**Be**	**Q**	Bao tên	**Ca-yeilth**
E	Nai	**Dzeh**	**R**	Thỏ	**Gah**
F	Cáo	**Ma-e**	**S**	Cừu	**Dibeh**
G	Dê	**Klizzie**	**T**	Gà tây	**Than-zie**
H	Ngựa	**Lin**	**U**	Ute	**No-da-ih**
I	Băng	**Tkin**	**V**	Người chiến thắng	**A-keh-di-glini**
J	Con lừa	**Tkele-cho-gi**	**W**	Chồn	**Gloe-ih**
K	Trẻ con	**Klizzie-yazzi**	**X**	Gạch chéo	**Al-an-as-dzoh**
L	Cừu non	**Dibeh-yazzi**	**Y**	Cây ngọc giá	**Tsah-as-zih**
M	Chuột	**Na-as-tso-si**	**Z**	Kẽm	**Besh-do-gliz**

Quân lực Nhật đã tấn công Trân Châu Cảng vào ngày 7 tháng Mười hai năm 1941, và không lâu sau khi họ chiếm được phần lớn phía tây Thái Bình dương, các đội quân của Nhật đã tràn tới nơi đồn trú của quân Mỹ ở Guam vào ngày 10 tháng Mười hai, họ chiếm Guadalcanal, một trong những hòn đảo thuộc quần đảo Solomon, vào ngày 13 tháng Mười hai, Hongkong đã đầu hàng vào ngày 25 tháng Mười hai và đội quân của Hoa Kỳ ở Phillipines cũng đầu hàng vào ngày 2 tháng Một năm 1942. Người Nhật định củng cố sự kiểm soát của mình trên vùng biển Thái Bình dương vào mùa hè năm sau bằng việc xây dựng một phi trường ở Guadalcanal dành cho máy bay ném bom, nhờ đó họ có thể chặn đứng đường tiếp tế quân nhu của quân Đồng minh, khiến cho

bất kỳ sự phản công nào của quân Đồng minh cũng đều không thể thực hiện được. Đô đốc Ernest King, Chỉ huy Chiến dịch Hải quân Mỹ, đã đốc thúc một cuộc tấn công vào hòn đảo trước khi phi trường được hoàn thành và ngày 7 tháng Tám, Sư đoàn Hải quân Thứ nhất đã dẫn đầu cuộc tấn công vào Guadalcanal. Trong số những người đầu tiên đổ bộ vào đảo có cả nhóm những người nói mật mã đầu tiên để chứng kiến trận đánh.

Mặc dù những người Navajo tự tin rằng năng lực của họ là một điềm phúc lành cho hải quân, song những nỗ lực ban đầu của họ chỉ gây nên sự lúng túng. Nhiều điện báo viên bình thường đã không biết mật mã mới này, và họ gửi những bức thư đầy hoảng loạn đi khắp hòn đảo, tuyên bố rằng Nhật Bản đã truyền tin trên các tần số của Mỹ. Viên đại tá chịu trách nhiệm việc này đã ngay lập tức cho ngừng liên lạc bằng mật mã Navajo cho đến khi ông thực sự tin rằng nó đáng để theo đuổi. Một trong những người nói mật mã nhớ lại mật mã Navajo cuối cùng cũng được sử dụng trở lại như thế nào:

> Viên đại tá đã có một ý tưởng. Ông nói ông sẽ giữ chúng tôi với một điều kiện: nếu tôi có thể thắng được "mật mã trắng" của ông - một thứ máy hình trụ kêu tích tắc. Cả hai chúng tôi đều gửi thư, ông thì bằng cái ống hình trụ màu trắng còn tôi thì bằng giọng nói. Cả hai chúng tôi đều nhận được thư trả lời và đua xem ai là người có thể giải mã sớm nhất. Người ta hỏi tôi: "Anh phải mất bao lâu? Hai giờ đồng hồ?" "Khoảng hơn 2 phút", tôi trả lời. Ông ta vẫn còn tiếp tục giải mã trong khi tôi đã xong khoảng 4 phút rưỡi rồi. Tôi nói: "Thưa đại tá, khi nào thì ông sẽ vứt bỏ cái thứ hình trụ này đi?". Ông ta không nói gì cả, chỉ châm tẩu thuốc rồi bỏ đi.

Những người nói mật mã đã nhanh chóng chứng tỏ giá trị của họ trên chiến trường. Trong suốt thời kỳ đầu trên đảo Saipan, một tiểu đoàn hải quân đã chiếm được các vị trí mà quân Nhật nắm giữ trước đây khiến họ phải rút quân. Bất ngờ một loạt súng vang lên gần đó. Họ bị tấn công bởi chính những đồng đội Mỹ của mình vì những người này không biết họ đã đi trước một bước. Đội hải quân đã truyền qua vô tuyến điện bằng tiếng Anh giải thích về vị trí của mình, song súng vẫn tiếp tục nổ vì các đội quân Mỹ này nghi ngờ rằng đây là thư của quân Nhật giả danh để lừa họ. Chỉ khi một bức thư bằng tiếng Navajo được truyền đi thì những kẻ tấn công mới nhận ra sai lầm của mình và ngừng bắn. Một bức thư Navajo không bao giờ có thể là giả và luôn tin tưởng được.

Danh tiếng của những người nói mật mã nhanh chóng lan truyền và vào cuối năm 1942, đã có yêu cầu thêm tám mươi ba người nữa. Navajo phải phục vụ cho tất cả sáu sư đoàn thuộc Quân đoàn Hải quân, và đôi khi còn được các lực lượng khác của Mỹ trưng dụng. Cuộc chiến về từ ngữ của họ nhanh chóng biến những người Navajo trở thành anh hùng. Những binh lính khác được lệnh phải mang vác máy vô tuyến điện và súng trường cho họ và họ thậm chí còn có lính bảo vệ riêng, một phần cũng là để bảo vệ đồng đội của họ. Có ít nhất ba trường hợp họ đã bị tưởng nhầm là quân Nhật và bị đồng đội Mỹ bắt giữ. Họ chỉ được thả ra sau khi được những đồng nghiệp của mình ở chính tiểu đoàn đó bảo lãnh.

Sự bất khả xâm phạm của mật mã Navajo hoàn toàn là nhờ vào thực tế là Navajo thuộc họ ngôn ngữ Na-Dene, không có dây mơ rễ má gì với bất kỳ ngôn ngữ nào ở châu Á cũng như châu Âu. Chẳng hạn, động từ Navajo được chia không chỉ phụ thuộc

vào chủ ngữ mà còn phụ thuộc cả vào bổ ngữ. Đuôi của động từ phụ thuộc vào loại của bổ ngữ: dài (ví dụ như ống, bút chì), thon dài và mềm dẻo (như con rắn, dây da), dạng hạt (như đường, muối), dạng bó (như rơm), nhớt (như bùn, phân) và nhiều loại khác nữa. Động từ cũng sẽ cấu thành trạng từ và thể hiện là người nói có chứng kiến sự việc mà anh ta hoặc cô ta đang nói đến, hay chỉ là tin đồn. Vì vậy, một động từ đơn có thể tương đương với cả một câu, khiến cho người nước ngoài thực sự không thể hiểu được nghĩa của nó.

Hình 52. Hai mươi chín người nói mật mã Navajo đầu tiên xếp hàng để chụp bức hình tốt nghiệp truyền thống.

Mặc dù có sức mạnh như vậy song mật mã Navajo vẫn có hai sơ hở cơ bản. Thứ nhất, các từ không nằm trong từ vựng Navajo cũng như trong danh sách 274 từ mật mã phải được đánh vần

bằng cách sử dụng bảng chữ cái đặc biệt. Điều này tốn khá nhiều thời gian, vì vậy người ta quyết định bổ sung thêm 234 từ thông thường nữa vào bảng từ vựng. Chẳng hạn, tên các quốc gia được đặt biệt hiệu Navajo: "Mũ xoay" tức là Australia, "Giới hạn bởi nước" là Anh, "Tóc tết bím" là Trung quốc, "Mũ sắt" là Đức, "Đất nổi" là Philippines,...

Vấn đề thứ hai liên quan đến những từ mà vẫn phải đánh vần. Nếu người Nhật nghe rõ các từ này được đánh vần như thế nào thì họ sẽ biết họ có thể sử dụng phương pháp phân tích tần suất để xác định các từ Navajo biểu thị cho những chữ cái nào. Sẽ nhanh chóng nhận ra ngay là từ sử dụng thường xuyên nhất là từ **dzeh**, có nghĩa là *elk* (nai) và tức là biểu thị chữ cái **e**, chữ cái thông dụng nhất trong bảng chữ cái tiếng Anh. Chỉ việc đánh vần tên của đảo Guadalcanal và việc lặp lại bốn lần từ **wol-la-chee** *(ant* - kiến) chính là một đầu mối lớn cho thấy từ này biểu thị chữ cái **a**. Giải pháp cho vấn đề này là sử dụng nhiều từ thay thế (từ đồng âm) cho các chữ cái được sử dụng thường xuyên. Người ta thêm hai từ thay thế nữa cho mỗi chữ cái trong 6 chữ cái thông dụng nhất (**e, t, a, o, i, n**), và một từ nữa cho sáu chữ cái thông dụng nhất tiếp theo (**s, h, r, d, l, u**). Chẳng hạn, chữ cái **a**, còn có thể được thay thế bằng từ **be-la-sana** *(apple* - táo) hay **tse-nihl** *(axe* - rìu). Sau đó, từ Guadalcanal được đánh vần chỉ bị lặp lại một lần: **klizzie, shi-da, wol-la-chee, lha-cha-eh, be-la-sana, dibeh-yazzie, moasi, tse-nihl, nesh-chee, tse-nihl, ah-jad** *(goat, uncle, ant, dog, apple, lamb, cat, axe, nut, axe, leg* - dê, bác, kiến, chó, táo, cừu non, mèo, rìu, hạt, rìu, chân).

Vì cuộc chiến ở Thái Bình dương trở nên dữ dội, và vì người Mỹ đã tiến quân đến Okinawa từ quần đảo Solomon, nên những

người nói mật mã Navajo ngày càng đóng một vai trò sống còn. Trong những ngày đầu tiên của cuộc tấn công vào Iwo Jima, hơn tám trăm bức thư Navajo đã được gửi đi, tất cả đều không có một sai sót nào. Theo Thiếu tá Howard Conner, "nếu không có những người Navajo, hải quân sẽ không bao giờ chiếm được Iwo Jima". Sự đóng góp của những người nói mật mã Navajo lại càng đáng kể hơn nếu bạn biết rằng, để hoàn thành nhiệm vụ của mình, họ thường phải đương đầu và tự vượt qua những nỗi sợ hãi sâu sắc về mặt tinh thần. Người Navajo tin rằng linh hồn của những người chết, *chindi*, sẽ trả thù những người sống nếu không có những nghi lễ trên xác chết. Mặt trận Thái Bình dương đặc biệt đẫm máu, với những xác chết rải rác khắp nơi trên chiến trường, và vì vậy những người nói mật mã phải tập trung hết mọi can đảm để làm việc bất chấp những *chindi* săn đuổi họ. Trong cuốn sách *Những người nói mật mã Navajo* của Doris Paul, một trong những người Navajo nhớ lại một sự việc biểu hiện điển hình cho lòng dũng cảm, sự cống hiến và tinh thần bình tĩnh của họ:

> Nếu bạn nhô cao đầu mình lên 6 inch thì bạn sẽ "đi toi" ngay, vì đạn lửa dày đặc. Và sau đó trong những giờ ít ỏi lại là một sự yên lặng chết chóc, không một chút bình yên cho cả bên ta hay bên địch. Nó đã khiến cho một người Nhật không thể chịu đựng thêm được nữa. Anh ta bật dậy và gào thét đến lạc giọng và lao về phía hào của chúng tôi, huơ lên một thanh kiếm samurai dài. Tôi nghĩ anh ta bị bắn khoảng hai mươi lăm đến bốn mươi lần trước khi ngã xuống.
>
> Một người bạn thân ở chung hào với tôi. Nhưng người Nhật đã cắt ngang họng anh ấy, xuyên qua dây thanh âm ở phía sau cổ. Anh ấy vẫn còn thở hổn hển ở thanh quản. Và cái âm thanh

khi anh ấy cố hít thở thật là khủng khiếp. Tất nhiên là anh ấy chết. Khi bọn chó Nhật tấn công, máu nóng bắn toé lên khắp bàn tay cầm ống nghe của tôi. Tôi đã kêu cứu bằng mật mã. Họ nói rằng bất chấp những gì xảy ra, mọi âm tiết trong thư của tôi đều vẫn rất rành rọt.

Tất cả đã có bốn trăm hai mươi người nói mật mã Navajo. Mặc dù lòng dũng cảm trong chiến đấu của họ được biết đến song vị trí đặc biệt của họ trong liên lạc bí mật thì không được phổ biến rộng rãi. Chính phủ cấm họ không được nói về nhiệm vụ của mình và sự đóng góp độc nhất vô nhị của họ không được công

Hình 53 Hạ sĩ Henry Bake, Jr. (trái) và binh nhất George H. Kirk đang sử dụng mật mã Navajo trong khu rừng rậm ở Bougainville vào năm 1943.

bố. Cũng như Turing và các nhà giải mã ở Bletchley Park, người Navajo bị lãng quên trong nhiều thập kỷ. Cuối cùng, vào năm 1968, mật mã Navajo đã được công bố và vào năm sau đó, những người nói mật mã đã có cuộc tái ngộ lần đầu tiên. Sau đó, vào năm 1982, họ đã rất vinh dự khi Chính phủ Mỹ lấy ngày 14 tháng Tám là "Ngày Quốc gia những người nói mật mã Navajo". Tuy nhiên, sự ban thưởng lớn nhất cho công việc của những người Navajo là một thực tế đơn giản: mật mã của họ là một trong số ít những mật mã chưa bao giờ bị phá vỡ trong lịch sử. Trung tướng Seizo Arisue, cục trưởng Cục tình báo Nhật Bản, đã thừa nhận rằng, mặc dù họ đã hóa giải được mật mã của Không lực Hoa Kỳ, song lại thất bại hoàn toàn trước mật mã Navajo.

Giải mã những ngôn ngữ đã biến mất và văn tự cổ

Thành công của mật mã Navajo phần lớn dựa trên thực tế đơn giản là tiếng mẹ đẻ của người này là hoàn toàn vô nghĩa với bất kỳ ai không quen thuộc với nó. Trên nhiều phương diện thì nhiệm vụ mà những nhà giải mã Nhật Bản phải đương đầu cũng tương tự như với các nhà khảo cổ học tìm cách giải mã một ngôn ngữ đã bị quên lãng từ lâu, có thể được viết trong một văn tự đã quá cổ xưa. Nếu có gì khác chăng thì đó là thử thách của các nhà khảo cổ học khắc nghiệt hơn rất nhiều. Chẳng hạn, nếu người Nhật Bản còn có được một dòng chảy liên tục các từ Navajo mà họ phải tìm cách giải mã thì thông tin sẵn có cho các nhà khảo cổ học đôi khi chỉ là một vài tấm đất sét. Hơn nữa, các nhà giải mã khảo cổ thường không có ý niệm gì về bối cảnh cũng như nội dung của một văn bản cổ, vốn là những

đầu mối mà các nhà giải mã quân sự thường dựa vào để giúp họ phá vỡ một mật mã.

Giải mã các văn bản cổ dường như là một sự theo đuổi gần như vô vọng, song có rất nhiều người, cả nam lẫn nữ, đã cống hiến bản thân mình cho nhiệm vụ khó khăn này. Sự ám ảnh của họ đã được dẫn dắt bởi khát vọng muốn hiểu được những văn bản viết tay của tổ tiên chúng ta, cho phép chúng ta nói được ngôn ngữ của họ và nắm bắt được một chút ít về tư tưởng và cuộc sống của họ. Có lẽ sự khao khát muốn giải mã những văn tự cổ đã được Maurice Pope tóm tắt hay nhất trong cuốn *Câu chuyện về giải mã* của ông: "Giải mã cho đến nay là những thành tựu hấp dẫn nhất của học thuật. Có một cái gì đó thần diệu ở những văn bản viết tay bí ẩn, đặc biệt là khi nó đến từ quá khứ xa xôi, và một vinh quang tương xứng sẽ dành cho người đầu tiên mở ra sự bí ẩn của nó."

Việc giải mã các văn tự cổ không nằm trong cuộc chiến diễn ra liên tục giữa các nhà tạo mã và giải mã, vì mặc dù cũng có những nhà giải mã với tư cách là các nhà khảo cổ học song không có các nhà tạo mã. Nói rõ hơn là, trong đa số trường hợp giải mã về ngôn ngữ, người viết không hề có chủ tâm che giấu ý nghĩa của văn tự. Vì vậy, phần còn lại của chương này, trình bày về vấn đề giải mã khảo cổ, sẽ hơi lạc ra khỏi chủ đề chính của cuốn sách một chút. Tuy nhiên, các nguyên tắc của giải mã khảo cổ về cơ bản cũng tương tự như trong giải mã quân sự truyền thống. Thực sự thì, rất nhiều nhà giải mã quân sự đã bị cuốn hút trước thách thức của một văn tự cổ chưa được vén màn bí mật. Điều này có thể là vì việc giải mã khảo cổ tạo nên một sự thay đổi dễ chịu so với việc giải mã quân sự, nó đem lại một câu đố thuần túy về trí

tuệ hơn là một thách thức quân sự. Nói cách khác, động cơ là vì tò mò, ham hiểu biết hơn là vì thù địch.

Nổi tiếng nhất, và có lẽ cũng lãng mạn nhất trong số tất cả các bản giải mã đó là hóa giải chữ viết tượng hình cổ Ai Cập. Trong nhiều thế kỷ, chữ viết tượng hình vẫn còn là một điều bí ẩn, và các nhà khảo cổ học không thể làm gì hơn là phỏng đoán về ý nghĩa của nó. Tuy nhiên, nhờ một cách giải mã cổ điển, chữ viết tượng hình cuối cùng cũng đã được giải mã và kể từ đó các nhà khảo cổ học đã đọc được những bản tường thuật trực tiếp về lịch sử, văn hóa và tín ngưỡng của người Ai Cập cổ đại. Việc giải mã chữ viết tượng hình đã nối liền thiên niên kỷ chúng ta với nền văn minh của các pharaon.

Chữ viết tượng hình cổ nhất xuất hiện vào năm 3000 trước công nguyên, và dạng chữ viết hoa mỹ này tồn tại trong suốt ba ngàn năm rưỡi sau đó. Mặc dù các ký hiệu phức tạp trong chữ viết tượng hình là lý tưởng cho các bức tường của những đền thờ trang nghiêm (tiếng Hy Lạp từ *hieroglyphica* có nghĩa là "những hình chạm khắc linh thiêng"), song chúng lại quá phức tạp để bám sát những giao dịch thường ngày. Vì vậy, phát triển song song với các chữ viết tượng hình là chữ *hieratic*, một dạng chữ viết sử dụng hằng ngày trong đó mỗi biểu tượng trong chữ viết tượng hình được thay thế bằng một biểu thị ước lệ, nhanh và dễ viết hơn. Vào khoảng năm 600 trước công nguyên, chữ *hieratic* được thay thế bằng thứ chữ viết thậm chí còn đơn giản hơn nữa được gọi là *demotic* (chữ viết bình dân), cái tên này có xuất xứ từ tiếng Hy Lạp *demotika* có nghĩa là "dân dã", để biểu thị tính năng thông dụng của nó. Chữ viết tượng hình, chữ *hieratic* và chữ viết bình dân về cơ bản là giống nhau - người

ta hầu như coi chúng đơn giản chỉ là những phông chữ khác nhau mà thôi.

Tất cả ba dạng chữ viết này đều theo ngữ âm, tức là các ký tự phần lớn đều biểu thị những âm khác nhau, cũng giống như trong bảng chữ cái tiếng Anh. Trong hơn ba ngàn năm, những người Ai Cập cổ đại đã sử dụng các loại chữ viết này trong mọi phương diện của cuộc sống, như chúng ta sử dụng chữ viết ngày nay. Sau đó, đến cuối thế kỷ thứ 4 sau Công nguyên, trong vòng một thế hệ, các văn tự Ai Cập đã biến mất. Những tư liệu cuối cùng về chữ viết Ai Cập cổ được tìm thấy ở đảo Philae. Một dạng chữ viết tượng hình ở đền thờ được khắc vào năm 394 sau Công nguyên, và một mẩu đá khắc chữ bình dân được cho là vào năm 450. Sự lan rộng của Nhà thờ Thiên chúa chính là nguyên nhân gây ra sự biến mất của chữ viết Ai Cập, vì họ cấm sử dụng chúng để tiêu diệt tận gốc rễ bất kỳ mối liên hệ nào với quá khứ vô thần của người Ai Cập. Những chữ viết cổ được thay thế bằng chữ Coptic, một dạng chữ viết gồm hai mươi tư chữ cái lấy từ bảng chữ cái Hy Lạp bổ sung thêm sáu ký tự bình dân được sử dụng cho các âm Ai Cập không biểu thị được bằng tiếng Hy Lạp. Sự thống trị của chữ Coptic đã hoàn toàn đến nỗi khả năng đọc được chữ tượng hình, chữ *hieratic* và chữ bình dân đã biến mất. Ngôn ngữ Ai Cập cổ tiếp tục được nói và tiến hóa thành cái gọi là ngôn ngữ Coptic, song trong quá trình đó, cả ngôn ngữ và chữ viết Coptic đều bị thay thế bởi sự lan tràn của chữ viết Ả Rập vào thế kỷ thứ 11. Mối liên hệ cuối cùng về ngôn ngữ với các vương quốc Ai Cập cổ đại đã bị cắt đứt và sự hiểu biết cần thiết để đọc được những truyền thuyết về các pharaon cũng biến mất theo.

Mối quan tâm đến chữ viết tượng hình được đánh thức trở lại vào thế kỷ thứ 17 khi Giáo hoàng Sixtus V quy hoạch lại thành phố Rome, theo một hệ thống đại lộ mới, đang dựng các tháp bia mang về từ Ai Cập tại mỗi ngã tư. Các học giả đã cố gắng thử giải mã nghĩa của các chữ viết tượng hình trên các tháp bia song lại gặp khó khăn do một quan niệm sai lầm: không ai được chuẩn bị để chấp nhận rằng các chữ viết tượng hình này biểu thị cho một ký tự ngữ âm, hay ký âm. Ý tưởng về việc viết theo từng âm được cho là quá tiến bộ so với một nền văn minh cổ đại như vậy. Thay vào đó, các học giả thế kỷ 17 lại cho rằng các chữ viết tượng hình là những ký hiệu biểu ý - tức là các ký tự phức tạp này biểu thị cho toàn bộ một ý tưởng và chẳng qua chỉ là loại chữ viết bằng tranh nguyên thủy. Việc tin rằng chữ viết tượng hình đơn giản chỉ là chữ viết bằng tranh thậm chí còn phổ biến ở cả những người nước ngoài đến thăm Ai Cập vào thời mà chữ viết tượng hình vẫn còn là chữ viết thịnh hành. Diodorus Siculus, nhà sử học Hy Lạp thế kỷ thứ nhất trước Công nguyên đã viết:

> Giờ hóa ra là dạng các chữ cái của người Ai Cập mang hình dáng của tất cả các loài sinh vật, của chân tay trên cơ thể con người và của vật dụng hằng ngày... Chữ viết của họ không diễn đạt những ý tưởng định sẵn bằng cách kết hợp các âm tiết với nhau, mà bằng vẻ ngoài của những cái đã được sao chụp và bằng ý nghĩa ẩn dụ đã in dấu vào trí nhớ qua hoạt động thực tiễn... Vì vậy mà biểu tượng con diều hâu đối với họ là tất cả những gì xảy ra nhanh vì sinh vật này là loài nhanh nhất trong số các động vật có cánh. Và ý tưởng này được chuyển giao, thông qua những ẩn dụ thích hợp, cho tất cả những gì mau lẹ và những thứ phù hợp với tốc độ.

Dưới ánh sáng của những giải thích như vậy, thì có lẽ không có gì đáng ngạc nhiên khi mà các học giả thế kỷ 17 đã cố gắng giải mã các chữ viết tượng hình bằng cách diễn dịch mỗi biểu tượng thành một ý tưởng trọn vẹn. Chẳng hạn, vào năm 1652, tu sĩ dòng Tên người Đức Athanasius Kircher đã xuất bản một cuốn tự điển về những giải thích có tính phúng dụ nhan đề *Œdipus agyptiacus* và sử dụng nó để tạo ra một loạt những bản dịch lý thú và kỳ quặc. Một nhóm chữ viết tượng hình mà ngày nay chúng ta đã biết nó chỉ tên của pharaon Apries, đã được Kircher dịch thành: "Những lợi ích của Osiris thần thánh tìm được là nhờ các nghi lễ linh thiêng và chuỗi Genii, để có thể nhận được các lợi ích của sông Nile." Ngày nay các bản dịch của Kircher nghe thật nực cười, song ảnh hưởng của chúng đối với những người làm ra vẻ là nhà giải mã khác là rất to lớn. Kircher còn hơn cả một nhà Ai Cập học: ông đã viết một cuốn sách về khoa học mật mã, xây dựng một đài phun nước có âm nhạc, phát minh ra chiếc đèn kỳ lạ (tiền thân của điện ảnh), tự mình đi sâu vào miệng núi lửa Vesuvius và được mệnh danh là "cha đẻ của ngành núi lửa học". Vị tu sĩ dòng Tên được biết đến rộng rãi với tư cách là học giả được kính trọng nhất ở thời ông, và vì thế những tư tưởng của ông tất nhiên đã ảnh hưởng đến nhiều thế hệ các nhà Ai Cập học tương lai.

Một thế kỷ rưỡi sau Kircher, vào mùa hè năm 1798, những di tích cổ của người Ai Cập cổ đại lại được nghiên cứu trở lại khi Napoleon Bonaparte phái một đoàn gồm các nhà sử học, khoa học và những chuyên gia họa hình theo sau đoàn quân xâm lược của mình. Những chuyên gia này, hay "những con chó Bắc Kinh" như đám binh lính vẫn gọi họ như vậy, đã thực hiện một công việc to lớn, đó là lập bản đồ, vẽ, sao chép, đo đạc và ghi lại

tất cả những gì họ chứng kiến. Vào năm 1799, các học giả Pháp đã bắt gặp mặt một phiến đá nổi tiếng nhất trong lịch sử ngôn ngữ học, do một đội quân Pháp đồn trú tại đồn Julien ở thị trấn Rosetta vùng delta sông Nile, tìm thấy. Tốp lính này nhận được lệnh phải phá đổ một bức tường cổ để dọn đường mở rộng địa phận của đồn. Gắn bên trong bức tường là một tấm đá trên đó có rất nhiều chữ viết; cùng một đoạn văn bản được viết trên tấm đá ba lần: bằng chữ Hy Lạp, chữ viết bình dân và chữ viết tượng hình. Phiến đá Rosetta, như người ta gọi ngày nay, dường như tương đương với một *crib* trong khoa mật mã, chính là các *crib* đã từng giúp các nhà giải mã ở Bletchley Park hóa giải mật mã Enigma. Đoạn viết bằng chữ Hy Lạp, có thể đọc được dễ dàng, chính là một đoạn văn bản thường dùng để so sánh với bản mật mã bằng chữ viết bình dân và chữ viết tượng hình. Phiến đá Rosetta tiềm tàng là một phương tiện để khám phá ý nghĩa của các biểu tượng Ai Cập cổ đại.

Các học giả ngay lập tức nhận ra giá trị của phiến đá và gửi nó về Viện Quốc gia ở Cairo để nghiên cứu chi tiết hơn. Tuy nhiên, trước khi Viện có thể bắt tay vào nghiên cứu một cách nghiêm túc, thì quân đội Pháp lại thực sự đang ở bên bờ vực của sự thất bại trước lực lượng của Anh đang tiến đến gần. Người Pháp đã chuyển Phiến đá Rosetta từ Cairo đến Alexandria là nơi tương đối an toàn. Trớ trêu thay, khi quân Pháp cuối cùng đã đầu hàng, Điều XVI trong Hiệp ước Đầu hàng buộc chuyển giao tất cả những di sản cổ ở Alexandria cho quân Anh, trong khi những thứ ở Cairo lại được trả về cho Pháp. Năm 1802, phiến đá bazan màu đen vô giá (với kích thước cao 118 cm, rộng 77 cm và dày 30 cm, nặng 3/4 tấn) đã được gửi đến Portsmouth trên con tàu

HMS *L'Egytienne* và cùng năm đó nó được trưng bày ở Bảo tàng Anh, nơi nó vẫn còn được lưu giữ cho đến ngày nay.

Bản dịch tiếng Hy Lạp nhanh chóng tiết lộ rằng Phiến đá Rosetta là văn bản ghi lại một quyết định của đại hội đồng các giáo sĩ Ai Cập vào năm 196 trước Công nguyên. Văn bản này ghi lại các lợi ích mà pharaon Ptolemy ban cho thần dân Ai Cập và nêu chi tiết những tôn vinh mà các giáo sĩ, để đáp lại, dành cho pharaon. Chẳng hạn, họ tuyên bố rằng "một lễ hội hằng năm sẽ được dành cho Đức Vua Ptolemy vạn tuế, người được thần Ptah yêu quý, trong các đền thờ trên khắp mọi miền từ ngày thứ nhất của tháng ăn Thề (Troth) kéo dài năm ngày, họ sẽ đeo vòng hoa, dâng vật tế cúng và dâng rượu cùng những nghi thức thông thường khác". Nếu hai bản chữ viết còn lại cũng mang ý nghĩa tương tự thì việc giải mã chữ viết tượng hình và chữ viết bình dân là rất dễ dàng. Tuy nhiên, vẫn còn ba trở ngại đáng kể. Thứ nhất, Phiến đá Rosetta đã bị hư hỏng nghiêm trọng, như có thể thấy ở Hình 54. Bản chữ viết Hy Lạp gồm 54 dòng, trong đó 26 dòng cuối cùng bị hư hỏng. Phần chữ viết bình dân có 32 dòng, trong đó 14 dòng đầu bị hư (cần lưu ý là chữ viết bình dân và chữ viết tượng hình được viết từ phải sang trái). Bản chữ viết tượng hình ở trong tình trạng tồi tệ nhất với nửa số dòng đã bị mất hoàn toàn và 14 dòng còn lại (tương đương với 28 dòng cuối cùng trong bản chữ viết Hy Lạp) cũng bị mất một phần. Trở ngại thứ hai đối với việc giải mã là hai văn tự Ai Cập chuyển tải ngôn ngữ Ai Cập cổ mà không còn ai sử dụng ít nhất là tám thế kỷ. Dù cho có thể tìm ra một tập hợp các biểu tượng Ai Cập tương ứng với một tập hợp các từ Hy Lạp, nhờ đó giúp cho các nhà ngôn ngữ học có thể hiểu được ý nghĩa của các biểu tượng Ai Cập, song

không thể thiết lập được âm của các từ Ai Cập. Trừ phi các nhà khảo cổ học biết được các từ Ai Cập được nói như thế nào, nếu không họ không thể xác định được ngữ âm của các biểu tượng. Cuối cùng, tài sản trí tuệ của Kircher vẫn khuyến khích các nhà khảo cổ coi chữ viết của người Ai Cập là một loại ký hiệu biểu ý, chứ không phải biểu âm, và vì vậy thậm chí rất ít người lưu tâm tới việc thử giải mã ngữ âm của chữ viết tượng hình.

Hình 54. Phiến đá Rosetta, được khắc vào năm 196 trước Công nguyên và được phát hiện vào năm 1799, có chứa những đoạn ký tự được viết bằng ba loại chữ viết khác nhau: chữ viết tượng hình ở trên cùng, ở giữa là chữ viết bình dân và dưới cùng là chữ Hy Lạp.

Một trong những học giả đầu tiên đặt nghi vấn đối với định kiến cho rằng chữ viết tượng hình là chữ viết bằng tranh, đó là nhà thông thái và thần đồng nước Anh, Thomas Young. Sinh năm 1773 tại Milverton, Somerset, Young biết đọc trôi chảy khi mới lên hai tuổi. Mười bốn tuổi, ông đã học tiếng Hy Lạp, Latin, Pháp, Ý, Do thái, Chalde, Syri, Samarita, Ả Rập, Ba Tư, Thổ Nhĩ Kỳ và Ethiopia, và khi là sinh viên của trường Emmanuel College, Cambridge, sự xuất sắc đã mang lại cho ông biệt hiệu là "Hiện tượng Young". Ở Cambridge, ông nghiên cứu y học song người ta nói rằng mối quan tâm của ông chỉ là những chứng bệnh chứ không phải là các bệnh nhân mà ông cứu chữa. Dần dần, ông bắt đầu tập trung hơn vào việc nghiên cứu và ít quan tâm hơn tới bệnh tật.

Young đã tiến hành hàng loạt những thí nghiệm y học khác thường, rất nhiều thí nghiệm trong số đó nhằm mục đích giải thích mắt người hoạt động như thế nào. Ông đã xác lập được rằng sự tri giác màu sắc là kết quả cảm nhận của ba loại cơ quan riêng biệt, mỗi loại nhạy cảm với một trong ba màu cơ bản. Sau đó, bằng cách đặt những vòng kim loại xung quanh một nhãn cầu sống, ông đã chứng minh được rằng việc điều chỉnh tiêu cự không đòi hỏi phải làm biến dạng cả con mắt mà chỉ do sự phồng xẹp của thủy tinh thể đóng vai trò là một thấu kính. Mối quan tâm của Young đến quang học đã dẫn ông đến với vật lý học, và một loạt những khám phá khác. Ông đã công bố bài báo *Lý thuyết sóng ánh sáng*, một bài báo kinh điển về bản chất của ánh sáng; ông cũng đã đưa ra một sự giải thích mới và tốt hơn về thủy triều; ông cũng là người đưa ra định nghĩa chính thức về năng lượng và đã công bố những bài báo xây dựng nền móng cho môn đàn hồi.

Thomas Young

Young dường như có thể giải quyết các vấn đề trong hầu hết các lĩnh vực, song điều này lại hoàn toàn không phải là lợi thế của ông. Trí não của ông quá dễ dàng bị lôi cuốn nên ông cứ nhảy từ đề tài này sang đề tài khác, bắt tay ngay vào một vấn đề mới trước khi làm xong cái cũ.

Khi Young nghe nói về Phiến đá Rosetta, nó đã trở nên một thách thức không thể cưỡng lại được. Vào mùa hè năm 1814, trong kỳ nghỉ hàng năm ở khu nghỉ mát bên bờ biển Worthing, ông có mang theo một bản sao của ba văn tự. Đột phá của Young nảy sinh khi ông tập trung nghiên cứu những chữ tượng hình được bao quanh bởi một vòng kín, được gọi là *cartouche*. Linh cảm của ông mách bảo rằng những chữ tượng hình này được bao quanh như vậy là vì chúng biểu thị một điều gì đó rất quan trọng, có thể là tên của pharaon Ptolemy, chẳng hạn, bởi vì tên viết theo chữ Hy Lạp của ông, Ptolemaios, có được nhắc đến trong đoạn văn bản viết bằng tiếng Hy Lạp. Nếu đúng là như vậy thì Young có thể khám phá ra ngữ âm của các chữ tượng hình tương ứng, vì tên của một pharaon được phát âm gần như nhau bất kể là theo ngôn ngữ nào. *Cartouche* Ptolemy được lặp lại sáu lần trên Phiến đá Rosetta, đôi khi theo cái gọi là phiên bản chuẩn, đôi khi

lại dài hơn và dụng công hơn. Young giả định rằng kiểu dài hơn là tên của Ptolemy kèm theo tước hiệu, vì vậy ông tập trung vào các biểu tượng xuất hiện trong phiên bản chữ chuẩn, để dự đoán giá trị âm tiết của mỗi chữ tượng hình (Bảng 13).

Bảng 13 Giải mã của Young đối với , *cartouche* Ptolemaios (phiên bản chuẩn) trên Phiến đá Rosetta

Chữ tượng hình	Giá trị âm tiết của Young	Giá trị thực
	p	**p**
	t	**t**
	tùy chọn	**o**
	lo hay **ole**	**l**
	ma hoặc **m**	**m**
	i	**i** hoặc **y**
	osh hoặc **os**	**s**

Mặc dù vào lúc đó ông vẫn chưa biết, song Young đã cố gắng liên hệ hầu hết các chữ tượng hình với những giá trị âm tiết đúng của nó. May mắn là ông đã đặt hai chữ tượng hình đầu tiên (,), chữ nọ ở trên chữ kia, theo đúng trật tự ngữ âm của chúng. Các viên thư lại đã đặt các chữ tượng hình theo kiểu này là vì những lý do thẩm mỹ, với cái giá phải trả là mất đi sự rõ ràng về ngữ âm. Họ thiên về cách viết này cốt là để tránh những khoảng trống và giữ được sự hài hòa đối với thị giác; đôi khi họ thậm chí còn hoán đổi vòng quanh các chữ cái theo hướng ngược hẳn với bất kỳ cách viết theo từng âm hợp lý nào, cũng chỉ cốt để tăng thêm vẻ đẹp của chữ viết. Sau khi giải mã được các chữ này, Young đã khám phá thêm một vòng kín *cartouche* nữa trong một

văn tự được chép lại từ đền Karnak ở Thebes mà ông ngờ rằng đó là tên một hoàng hậu của Ptolemy, Berenika (hay Berenice gì đó). Ông lặp lại phương pháp trước đó của mình và kết quả được trình bày ở Bảng 14.

Bảng 14 Giải mã của Young đối với , *cartouche* Berenika, ở đền thờ Karnak

Chữ tượng hình	Giá trị âm tiết của Young	Giá trị thực
	bir	**b**
	e	**r**
	n	**n**
	i	**i**
	tùy chọn	**k**
	ke hoặc **ken**	**a**
	vĩ tố giống cái	vĩ tố giống cái

Trong số 13 chữ tượng hình trong cả hai *cartouche*, Young đã xác định chính xác một nửa, và một phần tư là đúng một phần. Ông cũng xác định chính xác ký hiệu vĩ tố (ký hiệu cuối cùng) chỉ giống cái, đặt sau tên của các nữ hoàng và nữ thần. Mặc dù ông không thể biết được mức độ thành công của mình, song sự xuất hiện của () ở cả hai *cartouche*, cùng biểu thị chữ cái **i** trong cả hai trường hợp, cũng đã cho Young thấy rằng ông đã đi đúng hướng, và cho ông đầu mối cần thiết để tiếp tục giải mã. Tuy nhiên, công việc của ông đã đột ngột dừng lại. Dường như ông đã quá sùng bái lý luận của Kircher, cho rằng các chữ tượng hình chỉ là những ký hiệu biểu ý, và ông vẫn chưa sẵn sàng để phá vỡ hình mẫu tư duy này. Ông đã tự bào chữa cho chính những

khám phá của mình bằng nhận xét rằng triều đại Ptolemy được truyền lại từ Lagus, một vị tướng của Alexander Đại đế. Nói cách khác, dòng họ Ptolemy là những người nước ngoài và Young đưa ra giả thuyết rằng tên của họ có lẽ đã được viết theo từng âm vì không có một ký hiệu biểu ý tự nhiên nào trong các chữ tượng hình ở phiên bản chuẩn. Ông đã tóm tắt lại những ý tưởng của mình bằng việc so sánh chữ tượng hình với các ký tự Trung Hoa, mà những người châu Âu chỉ mới bắt đầu hiểu được:

> Thật cực kỳ thú vị nếu ta theo dõi các bước xuất hiện của chữ viết theo bảng chữ cái từ cách viết tượng hình; một quá trình có thể được minh họa bằng cách thức mà tiếng Trung Hoa hiện đại biểu thị một tổ hợp các âm tiếng nước ngoài, các ký tự này được hoàn lại tính "ngữ âm" đơn giản bằng một ký hiệu thích hợp, mà không giữ lại ý nghĩa tự nhiên của chúng; và ký hiệu này, trong một số cuốn sách in hiện đại, đã rất gần với vòng kín bao quanh các tên viết bằng chữ tượng hình.

Young gọi thành quả của mình là "trò tiêu khiển trong một vài giờ rảnh rỗi". Ông đã mất hứng thú với chữ tượng hình cổ và kết thúc công việc của mình bằng một bài báo tóm tắt in trong Phụ lục của cuốn bách khoa thư *the Encyclopedia Britannica* năm 1819.

Trong khi đó ở Pháp, một nhà ngôn ngữ học trẻ tuổi đầy hứa hẹn, Jean-Franois Champollion, đã sẵn sàng để đưa các ý tưởng của Young đến kết luận tự nhiên của chúng. Mặc dù chưa tới ba mươi tuổi, song Champollion đã bị những chữ tượng hình cuốn hút gần như suốt hai thập kỷ. Sự lôi cuốn này bắt đầu vào năm 1800 khi nhà toán học người Pháp Jean-Baptiste Fourier, một trong những "con chó Bắc Kinh" đầu tiên của Napoleon giới thiệu

Jean-François Champollion

cho cậu bé Champollion 10 tuổi về bộ sưu tập đồ cổ Ai Cập của mình, rất nhiều trong số đó được trang trí bởi những chữ viết kỳ lạ. Fourier đã giải thích rằng không ai có thể dịch được thứ chữ viết bí ẩn này, lúc đó, cậu bé đã hứa là một ngày nào đó cậu sẽ giải mã được điều bí ẩn đó. Chỉ bảy năm sau, ở tuổi 17, cậu đã cho công bố bài báo với nhan đề *Ai Cập dưới thời các pharaon*. Ngay lập tức cậu được bầu vào Viện Hàn lâm ở Grenoble. Khi nghe tin mình trở thành một giáo sư tuổi chưa đầy hai mươi, Champollion đã choáng váng đến mức ngất xỉu.

Champollion tiếp tục khiến cho những người cùng thời của ông phải kinh ngạc trước sự tinh thông các ngôn ngữ như Latin, Hy Lạp, Hebrew, Ethiopi, Sanskrit (chữ Phạn), Zend, Pahlevi, Ả rập, Syri, Chaldean, Ba Tư và Trung Hoa của ông, tất cả đều nhằm trang bị cho cuộc tấn công vào chữ tượng hình. Minh chứng cho sự ám ảnh này của ông là câu chuyện xảy ra vào năm 1808 khi ông tình cờ gặp một người bạn cũ trên đường phố. Người bạn này ngẫu nhiên có nhắc đến Alexandre Lenoir, một nhà Ai Cập học nổi tiếng, mới công bố một bản giải mã hoàn chỉnh các chữ tượng hình. Champollion sốc đến mức sụp ngã

ngay tại chỗ (dường như ông này cũng rất có tài ngất xỉu). Cứ như là toàn bộ lý do để ông sống trên cõi đời này là phải trở thành người đầu tiên đọc được chữ viết của người Ai Cập cổ đại không bằng. May mắn cho Champollion, bản giải mã của Lenoir cũng kỳ quặc như những nỗ lực của Kircher ở thế kỷ 17, và thách thức vẫn còn đó.

Năm 1822, Champollion áp dụng phương pháp của Young cho các *cartouche* khác. Nhà tự nhiên học người Anh W. J. Bankes đã mang một tháp bia trên đó có khắc chữ tượng hình và chữ Hy Lạp đến Dorset, và sau đó đã cho in thạch bản các chữ viết song ngữ này, trong đó có các vòng kín bao quanh tên của Ptolemy và Cleopatra. Champollion đã có bản in này và cố gắng thiết lập các giá trị có nghĩa cho từng chữ riêng biệt (Bảng 15). Các chữ cái **p, t, o, l** và **e** thường xuất hiện trong cả hai cái tên này; trong bốn trường hợp, chúng đều được biểu thị bởi cùng một chữ tượng hình trong tên của Ptolemy và Cleopatra, chỉ có mỗi trường hợp **t** là có sự không nhất quán. Champollion giả định rằng âm **t** có thể được biểu thị bởi hai chữ tượng hình, giống như âm **c** trong tiếng Anh có thể được biểu thị bằng chữ **c** hoặc chữ **k**, như trong các từ *cat* và *kid*. Hứng khởi trước thành công của mình, Champollion bắt đầu tiếp cận các *cartouche* không có bản dịch song ngữ, bằng cách thay thế những giá trị âm mà ông thu được từ các *cartouche* Ptolemy và Cleopatra. *Cartouche* bí ẩn đầu tiên của ông (Bảng 16) có chứa một trong những cái tên vĩ đại nhất thời cổ đại. Theo Champollion thì rõ ràng *cartouche* này, đọc là **a-l-?-s-e-?-t-r-?**, biểu thị một cái tên - **alksentrs** - tức Alexandros theo tiếng Hy Lạp, hay Alexander theo tiếng Anh. Cũng rõ ràng đối với Champollion là người viết bản thảo này không thích sử

dụng nguyên âm, và thường bỏ qua chúng; có lẽ người viết cho rằng người đọc sẽ chẳng khó khăn gì trong việc thêm vào những nguyên âm bị mất. Với hai bản chữ tượng hình mới trong tay, nhà học giả trẻ tuổi đã nghiên cứu các đoạn chữ viết mới và giải mã được một loạt *cartouche* khác. Tuy nhiên, tất cả những tiến triển này mới đơn giản chỉ là mở rộng thêm các thành quả của Young. Những cái tên như Alexander và Cleopatra vẫn là những cái tên nước ngoài, vì vậy điều này chỉ hỗ trợ thêm cho thuyết xem rằng ngữ âm chỉ được viện đến để dùng cho những từ nằm ngoài từ vựng truyền thống của người Ai cập.

Bảng 15. Bản giải mã của Champollion [illegible] và [illegible] các *cartouche* Ptolemaios và Cleopatra từ tháp bia của Bankes.

Chữ tượng hình	Giá trị âm	Chữ tượng hình	Giá trị âm
	p		c
	t		l
	o		e
	l		o
	m		p
	e		a
	s		t
			r
			a

Sau đó, vào ngày 14 tháng Chín năm 1822, Champollion nhận được những bản chạm nổi từ đền thờ Abu Simbel, trong đó có chứa các *cartouche* có niên đại trước thời kỳ thống trị của La Mã - Hy Lạp. Điều quan trọng của những *cartouche* này là ở chỗ chúng đủ cổ xưa để có chứa trong đó những cái tên Ai Cập truyền thống, song chúng vẫn được viết theo từng âm - bằng chứng rõ ràng

chống lại thuyết cho rằng việc viết theo từng âm chỉ áp dụng cho các tên nước ngoài. Champollion đã tập trung vào một *cartouche* chỉ chứa có bốn chữ tượng hình . Hai ký hiệu đầu tiên chưa biết, song cặp chữ được lặp lại ở cuối, đã được biết từ *cartouche* Alexander (**alksentrs**) cả hai đều biểu thị chữ **s**. Điều này có nghĩa là *cartouche* này biểu thị chữ (**?-?-s-s**). Ở đây, Champollion đã vận dụng kiến thức uyên bác về ngôn ngữ của mình. Mặc dù Coptic, một hậu duệ trực tiếp của ngôn ngữ Ai Cập cổ đại, đã không còn là một sinh ngữ vào thế kỷ 11 sau Công nguyên, nhưng nó vẫn tồn tại dưới dạng "hóa thạch" trong các nghi lễ của Nhà thờ Coptic Thiên chúa. Champollion đã học ngôn ngữ Coptic khi còn là thiếu niên và thuần thục đến mức sử dụng chúng để ghi nhật ký. Tuy nhiên, mãi cho đến lúc này, ông mới nhận ra rằng Coptic cũng có thể là ngôn ngữ của các chữ tượng hình.

Bảng 16. Giải mã của Champollion đối với *cartouche* Alksentrs (Alexander).

Chữ tượng hình	Giá trị âm
	a
	l
	k
	s
	e
	?
	t
	r
	n

Champollion tự hỏi liệu ký hiệu đầu tiên trong *cartouche* đó, ( ), có phải là một ký hiệu biểu ý chỉ mặt trời, tức là, một bức vẽ mặt trời chính là ký hiệu cho từ "mặt trời". Sau đó, với trực giác thiên tài, ông cho rằng giá trị âm của ký hiệu biểu ý này chính là âm của một từ trong tiếng Coptic chỉ mặt trời, đó là từ **ra**. Nó cho ông kết quả là (**ra-?-s-s**). Chỉ có tên của một pharaon là dường như thích hợp. Chấp nhận sự bỏ qua nguyên âm rất khó chịu này và giả định chữ cái còn lại là **m**, thì chắc chắn đây phải là cái tên Rameses, một trong những pharaon vĩ đại nhất và cũng là một trong những cái tên cổ xưa nhất. Như vậy ngay cả những cái tên truyền thống cổ đại cũng được viết theo từng âm. Champollion đã lao vào văn phòng của người anh và kêu lên "Je tiens l'affaire!" *(Em đã thành công rồi)*, và một lần nữa, ông lại không chế ngự nổi niềm đam mê mãnh liệt của mình đối với chữ tượng hình. Ông ngay lập tức ngất xỉu và phải nằm bẹp trên giường suốt năm ngày sau đó.

Champollion cũng đã chứng minh được rằng người chép bản thảo đôi khi cũng khai thác nguyên tắc đánh đố bằng tranh vẽ, mà ta vẫn còn thấy trong các câu đố dành cho trẻ em. Cụ thể, các từ dài bị tách ra thành các thành phần ngữ âm, rồi sau đó được biểu thị bằng các ký hiệu biểu ý. Ví dụ, từ *belief* có thể được tách thành hai âm tiết, *be-lief*, sau đó được viết lại thành *bee-leaf*. Thay vì viết các từ này bằng các chữ cái, chúng lại được biểu thị bằng hình ảnh một con ong *(bee)* tiếp theo đó là một chiếc lá *(leaf)*. Trong ví dụ được Champollion khám phá, chỉ có âm tiết đầu tiên (**ra**) là được biểu thị bằng một câu đố bằng tranh (một hình vẽ mặt trời), trong khi phần còn lại của từ lại được viết từng âm theo cách thông thường.

Tầm quan trọng của ký hiệu biểu ý mặt trời trong *cartouche* Rameses là vô cùng to lớn, vì rõ ràng là nó đã hạn chế phạm vi các thứ ngôn ngữ mà người chép bản thảo có thể nói. Chẳng hạn, người này không thể nói tiếng Hy Lạp, vì nếu không, *cartouche* này sẽ phải được phát âm là "helios-meses". *Cartouche* này chỉ có nghĩa khi người chép nói thứ ngôn ngữ Coptic, vì khi đó nó mới được phát âm thành "ra-meses".

Mặc dù đây chỉ là một *cartouche* nữa song bản giải mã này đã chứng minh một cách rõ ràng bốn nguyên lý cơ bản của chữ tượng hình. Thứ nhất, ngôn ngữ của bản thảo ít nhất có liên quan đến tiếng Coptic, và thực sự thì việc khảo sát các văn bản chữ tượng hình khác cũng cho thấy đó là ngôn ngữ Coptic thuần khiết và đơn giản. Thứ hai, các ký hiệu biểu ý được sử dụng để biểu thị một số từ, ví dụ, từ "mặt trời" được biểu thị bởi một hình vẽ đơn giản về mặt trời. Thứ ba, toàn bộ hoặc một phần một số từ dài được tạo thành bằng cách dùng nguyên tắc đố tranh. Cuối cùng, trong hầu hết các bản thảo, những người viết đều dựa trên một bảng chữ cái ngữ âm tương đối quen thuộc. Điểm cuối cùng này là điều quan trọng nhất và Champollion đã gọi ngữ âm là "linh hồn" của chữ viết tượng hình.

Sử dụng những kiến thức sâu rộng của mình về ngôn ngữ Coptic, Champollion đã bắt đầu giải mã suôn sẻ những chữ tượng hình phong phú ngoài các *cartouche*. Trong vòng hai năm, ông đã xác định giá trị ngữ âm của phần lớn các chữ tượng hình, và khám phá ra rằng một số chữ biểu thị sự kết hợp của hai hay thậm chí tới ba phụ âm. Điều này đôi khi cho phép người viết lựa chọn cách viết một từ bằng cách sử dụng một số chữ tượng hình đơn giản hoặc chỉ vài chữ tượng hình đa phụ âm.

Champollion thông báo kết quả ban đầu của mình trong một bức thư gửi Ngài Dacier, thư ký thường trực của Viện Hàn lâm Văn khắc *(Académie des Inscriptions)*. Sau đó, vào năm 1824, ở tuổi 34, Champollion đã cho xuất bản tất cả những thành tựu của ông trong cuốn sách có nhan đề *Giản yếu về hệ thống chữ tượng hình (Précis du système hiéoglyphique)*. Lần đầu tiên trong mười bốn thế kỷ, chúng ta đã có thể đọc được lịch sử của các pharaon, đúng như được viết bởi những viên thư lại của họ. Đối với các nhà ngôn ngữ học, đây là một cơ hội để nghiên cứu sự tiến triển của một ngôn ngữ và một thứ chữ viết qua một khoảng thời gian kéo dài hơn 3000 năm. Chúng ta đã có thể hiểu được chữ tượng hình và lần theo dấu tích của nó từ thiên niên kỷ thứ ba trước Công nguyên đến thế kỷ thứ tư sau Công nguyên. Hơn nữa, sự phát triển của chữ tượng hình có thể được so sánh với thứ chữ viết *hieratic* và chữ viết bình dân mà lúc đó cũng đã được giải mã.

Trong vài năm, chính trị và sự ghen tỵ đã khiến cho những thành quả tuyệt vời của Champollion không được chấp nhận rộng rãi. Thomas Young là người chỉ trích thậm tệ nhất. Trong một số lần, Young đã không thừa nhận chữ tượng hình chủ yếu là ngữ âm; nhưng lúc khác thì ông lại chấp nhận, song phàn nàn rằng chính ông đã đi đến kết luận này trước cả Champollion, và rằng người Pháp này chỉ lấp đầy những khoảng còn trống mà thôi. Phần lớn sự thù địch này của Young là do Champollion đã không chia sẻ cho ông một chút vinh dự nào mặc dù rõ ràng là những đột phá ban đầu của Young đã gợi ý cho sự giải mã hoàn chỉnh.

Tháng Bảy năm 1828, Champollion đã thực hiện chuyến thám hiểm đầu tiên tới Ai Cập kéo dài 18 tháng. Đó là một cơ hội lớn để ông thấy tận mắt những bản thảo mà ông mới chỉ nhìn thấy trên

các bản vẽ hoặc bản in thạch bản. Ba mươi năm trước, đoàn quân viễn chinh của Napoleon đã ước đoán một cách tùy tiện rằng ý nghĩa của những chữ tượng hình này chỉ là để trang hoàng cho các đền thờ, song giờ đây Champollion đã có thể đơn giản đọc chúng lên từng chữ một và dịch lại một cách chính xác. Chuyến viếng thăm của ông quả là rất đúng lúc. Ba năm sau, trong khi ghi chép lại những ghi chú, các bức vẽ và bản dịch từ chuyến đi Ai Cập, ông đã bị đột quỵ. Những cơn ngất mà ông phải chịu trong suốt cuộc đời có lẽ là triệu chứng của một căn bệnh nghiêm trọng hơn, lại càng nặng thêm bởi sự nghiên cứu đầy ám ảnh và căng thẳng của ông. Ông đã mất vào ngày 4 tháng Ba năm 1832 ở tuổi 41.

Bí mật của Linear B

Trong vòng hai thế kỷ sau đột phá của Champollion, các nhà Ai Cập học tiếp tục hoàn thiện những hiểu biết của họ về những phức tạp của chữ tượng hình. Trình độ hiểu biết của họ giờ đây cao đến mức mà các học giả có thể giải mã được thậm chí cả những chữ tượng hình đã được mã hóa của một trong những văn bản mật mã cổ xưa nhất thế giới. Một số văn tự tìm thấy trên những tấm bia mộ của các pharaon được mã hóa với các kỹ thuật rất đa dạng, bao gồm cả mật mã thay thế. Đôi khi người ta dùng cả các ký hiệu giả để thay thế cho chữ gốc, và trong một số trường hợp khác thì một chữ khác âm nhưng nhìn thì tương tự nhau được dùng thay cho chữ đúng. Chẳng hạn, chữ hình con rắn có mào, thường biểu thị chữ **f**, lại được sử dụng để thay thế cho chữ hình rắn, biểu thị chữ **z**. Thường thì các văn bia được mã hóa này cũng không có chủ định để không cho ai giải mã được mà chúng chỉ có vai trò như là những câu đố mật mã nhằm khơi

gợi sự tò mò của những khách qua đường, khiến họ nán lại bên ngôi mộ thay vì dửng dưng đi qua.

Sau khi chinh phục được các chữ tượng hình, các nhà khảo cổ tiếp tục giải mã rất nhiều các văn tự cổ khác, trong đó bao gồm cả chữ hình nêm của Babylon, cổ tự Kôk-Turki của Thổ Nhĩ Kỳ và bảng chữ cái Brahmi của Ấn Độ. Tuy nhiên, tin tốt lành cho những tài năng bắt đầu nảy nở như Champollion, đó là vẫn còn một số văn tự đang chờ khám phá, như các văn tự viết bằng ngôn ngữ Etruria (xưa thuộc Italia) và Indus (xem Phụ lục I). Khó khăn lớn trong việc giải mã các văn tự còn lại này là chúng không có các *crib*, không có gì giúp cho các nhà giải mã khai phá ý nghĩa của các văn bản cổ này. Với chữ tượng hình cổ Ai Cập thì các *cartouche* đóng vai trò như các *crib*, đã mang lại cho Young và Champollion cái hương vị đầu tiên về nền móng ngữ âm ẩn giấu phía sau. Không có các *crib*, việc giải mã một văn tự cổ dường như là vô vọng. Tuy nhiên, cũng có một ví dụ đáng phải kể đến về một thứ chữ viết đã được giải mã mà không cần có sự hỗ trợ của *crib*. Linear B, chữ viết của người Cret thuộc Thời kỳ Đồ đồng, đã được giải mã mà không có bất kỳ một manh mối trợ giúp nào do người viết cổ xưa để lại. Nó được giải quyết là nhờ sự kết hợp của logic và cảm hứng, một ví dụ có sức thuyết phục mạnh mẽ về sự giải mã thuần túy. Thực tế, việc giải mã Linear B đã được đông đảo mọi người coi là vĩ đại nhất trong tất cả những giải mã khảo cổ học.

Câu chuyện về Linear B bắt đầu từ những khai quật của Ngài Arthur Evans, một trong những nhà khảo cổ học kiệt xuất nhất vào lúc chuyển giao thế kỷ. Evans rất quan tâm đến thời kỳ lịch sử Hy Lạp được Homer mô tả trong hai bộ sử thi *Iliad* và *Odyssey*. Homer đã thuật lại cuộc Chiến tranh thành Troy, chiến thắng lẫy

lừng của quân Hy Lạp ở Troy và những kỳ công tiếp theo của người anh hùng Odysseus, những sự kiện được cho là diễn ra vào thế kỷ thứ 12 trước Công nguyên. Một số học giả thế kỷ 19 đã bác bỏ giả thuyết đó và coi các sử thi của Homer chẳng qua chỉ là huyền thoại, song vào năm 1872 nhà khảo cổ người Đức, Heinrich Schliemann đã khám phá ra vị trí của thành Troy, ở gần bờ biển phía đông Thổ Nhĩ Kỳ, và đột nhiên những câu chuyện thần thoại của Homer trở thành lịch sử. Vào giữa những năm 1872 và 1900, các nhà khảo cổ đã khám phá thêm nhiều bằng chứng về một thời kỳ thịnh vượng tiền Văn minh Hy Lạp, trước thời đại Hy Lạp cổ điển của Pythagoras, Plato và Aristotle khoảng 600 năm. Thời kỳ tiền Văn minh Hy Lạp kéo dài từ năm 2800 đến 1100 trước Công nguyên, và nó đã đạt tới đỉnh cao trong suốt bốn thế kỷ cuối cùng. Trên lục địa Hy Lạp mà trung tâm là Mycenae, các nhà khảo cổ học đã tìm thấy cả một mảng rộng lớn những đồ tạo tác và kho báu. Tuy nhiên, Ngài Arthur Evans đã rất băn khoăn khi thấy các nhà khảo cổ không tìm được bất kỳ dạng chữ viết nào. Ông không thể chấp nhận việc một xã hội phát triển cao đến như thế mà lại có thể hoàn toàn mù chữ, và quyết định chứng minh rằng nền văn minh Mycenae phải có một dạng chữ viết nào đó.

Sau khi gặp nhiều nhà buôn đồ cổ ở Athen, Ngài Arthur cuối cùng cũng đã tình cờ bắt gặp một số mẩu đá được chạm khắc. Dễ dàng nhận ra đó là những con dấu có niên đại từ thời tiền Văn minh Hy lạp. Những ký hiệu trên các con dấu đó có vẻ như chỉ là các biểu tượng chứ không phải là chữ viết thực, tương tự như hệ thống các ký hiệu trên các huy hiệu. Tuy nhiên, sự phát hiện này đã thúc đẩy ông tiếp tục truy tìm. Các con dấu này được cho là có xuất xứ từ đảo Crete, mà cụ thể là ở Knossos, nơi mà theo

truyền thuyết có cung điện của Vua Minoa, trung tâm của một đế chế thống trị toàn bộ vùng biển Aege. Ngài Arthur bèn lên đường đến đảo Crete và tiến hành khai quật vào năm 1900. Những kết quả thu được cũng ngoạn mục như tốc độ mau lẹ của chúng. Ông đã khám phá ra phần còn lại của một cung điện huy hoàng, với một hệ thống chằng chịt các hành lang và được trang hoàng bằng rất nhiều tấm bích họa vẽ những người đàn ông trẻ tuổi nhảy lên những con bò đực hung dữ. Evans xét đoán rằng môn thể thao cưỡi bò này phần nào có liên quan tới thần thoại về Nhân Ngưu, một con quái vật đầu bò có thân hình là của chàng thanh niên vạm vỡ, và ông cho rằng sự phức tạp của các lối đi trong cung điện là lấy cảm hứng từ câu chuyện về mê cung của con Nhân Ngưu này.

Hình 57 Các địa danh cổ xưa quanh biển Aege. Sau khi phát hiện các kho báu tại Mycenae trên lục địa Hy Lạp, Ngài Arthur Evans đã tiến hành tìm kiếm các bản khắc chữ viết. Những bản khắc chữ *Linear B* đầu tiên được tìm thấy trên đảo Crete, trung tâm của đế chế Minoa.

Ngày 31 tháng Ba, Ngài Arthur đã bắt đầu khai quật một kho báu mà ông mong đợi nhất. Đầu tiên chỉ là một tấm đất sét có chữ viết trên đó, rồi vài ngày sau là một cái rương bằng gỗ chứa đầy những tấm tương tự và sau nữa là những đống bản thảo còn hơn cả sự mong đợi của ông. Tất cả những bản khắc đất sét này xưa kia đã được phơi nắng cho khô, chứ không phải nung bằng lửa, vì vậy chúng có thể được sử dụng lại đơn giản bằng cách nhúng nước. Qua nhiều thế kỷ, mưa gió đã có thể làm tan rữa các tấm đất sét này và chúng có thể đã biến mất vĩnh viễn. Tuy nhiên, dường như cung điện ở Knossos đã bị lửa thiêu rụi, các tấm đất sét được nung chín và nhờ vậy mà chúng đã được bảo vệ trong suốt ba ngàn năm. Tất cả được giữ gìn tốt đến mức có thể phân biệt được cả dấu vân tay của người viết.

Các bản khắc đất sét này được phân làm ba nhóm. Nhóm thứ nhất, có niên đại từ năm 2000 đến 1650 trước Công nguyên, chỉ bao gồm các hình vẽ, mà cũng có thể là các ký hiệu biểu ý, nhìn bề ngoài dường như là có liên quan đến các ký hiệu trên các con dấu mà Ngài Arthur Evans đã mua được từ các nhà buôn ở Athens. Nhóm thứ hai, có niên đại từ năm 1750 đến 1450 trước Công nguyên, được khắc các ký tự gồm các vạch thẳng đơn giản, và vì vậy chữ viết này được đặt tên là Linear A *(linear* có nghĩa là thẳng, tuyến tính - ND). Nhóm thứ ba, có niên đại từ năm 1450 đến 1375 trước Công nguyên, mang chữ viết có vẻ như là một dạng cải tiến từ Linear A, và vì vậy được gọi là Linear B. Vì hầu hết các tấm đất sét đều là Linear B và vì đó là bản chữ viết mới nhất nên Ngài Arthur và các nhà khảo cổ khác tin rằng Linear B sẽ mang đến cho họ một cơ hội giải mã tốt nhất.

Rất nhiều tấm đất sét có chứa những bảng kiểm kê. Với nhiều

cột bao gồm các ký tự số, nên tương đối dễ dàng xác định được hệ thống đếm, song các ký hiệu ngữ âm thì lại khó hiểu hơn rất nhiều. Chúng giống như một tập hợp vô nghĩa những nét nguệch ngoạc khá tùy tiện. Nhà sử học David Kahn đã mô tả một vài ký hiệu riêng lẻ trông như "một mái vòm Gothic với một đường thẳng đứng, một chiếc thang, một trái tim với cái cuống lá xuyên qua, một chiếc đinh ba cong có ngạnh, một con khủng long ba chân ngoái nhìn ra phía sau, một chữ A với một thanh ngang xuyên qua, một chữ S lộn ngược, một ly bia cao, đầy một nửa, với một chiếc nơ buộc quanh miệng; và hàng tá những ký hiệu khác trông chẳng giống thứ gì cả". Chỉ có hai sự thực hữu ích được xác lập về Linear B. Thứ nhất là hướng viết rõ ràng là từ trái sang phải, vì những chỗ hụt ở cuối một dòng thường ở phía bên phải. Thứ hai, có chín mươi ký tự khác nhau, chứng tỏ chữ viết gần như chắc chắn là theo âm tiết. Các chữ viết thuần túy theo bảng chữ cái thì đều có xu hướng có khoảng từ 20 đến 40 ký tự (chẳng hạn như tiếng Nga có 36 ký hiệu, còn chữ ả rập là 28). Ở thái cực khác, những chữ viết dựa trên ký hiệu biểu ý thì thường có đến hàng trăm hoặc thậm chí hàng ngàn ký hiệu (tiếng Trung Quốc có hơn 5000 ký hiệu). Các chữ viết theo âm tiết nằm trung gian, có khoảng từ 50 đến 100 ký tự âm tiết. Ngoài hai sự thực này, thì Linear B vẫn là một bí ẩn không thể hiểu được.

Vấn đề cơ bản là không ai biết chắc là Linear B được viết bằng ngôn ngữ gì. Ban đầu có người phỏng đoán Linear B là một dạng chữ viết Hy Lạp, vì có bảy ký tự rất tương đồng với các ký tự trong chữ viết Cypriot kinh điển vốn được biết là một dạng chữ viết mà người Hy Lạp đã sử dụng trong khoảng từ năm 600 đến 200 trước Công nguyên. Song những nghi ngờ bắt đầu nảy sinh.

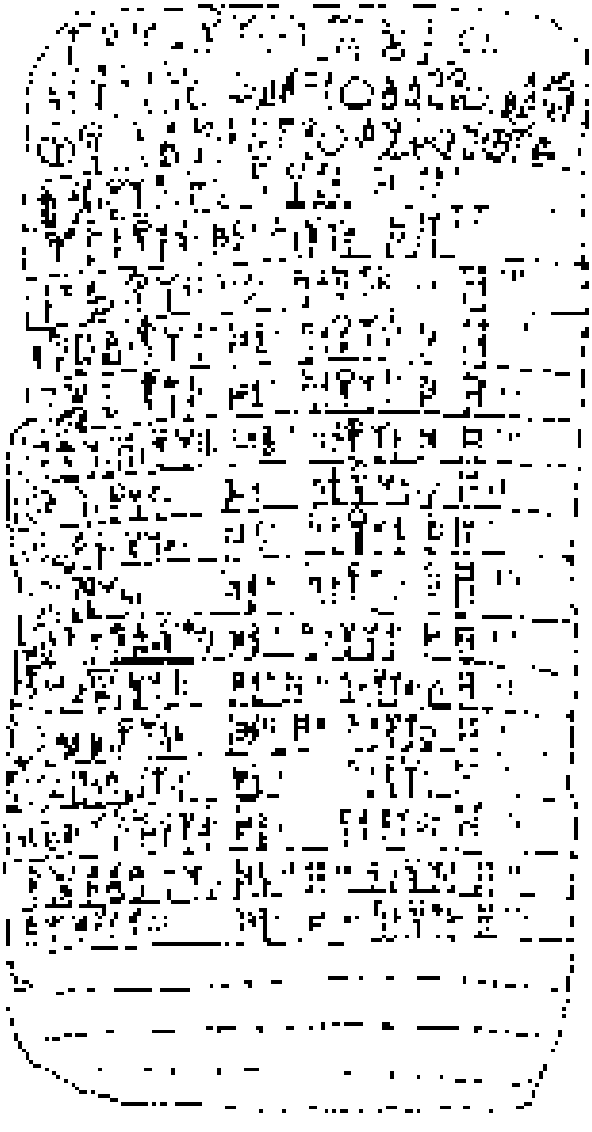
Phụ âm cuối thường thấy nhất trong tiếng Hy Lạp là **s**, và do đó ký tự cuối cùng thông dụng nhất trong chữ viết Cypriot là , biểu thị âm tiết **se** - bởi vì các ký tự là theo âm tiết, nên một phụ âm đơn phải được biểu thị bởi một kết hợp phụ âm-nguyên âm, nhưng phải là nguyên âm câm. Chính ký tự này cũng xuất hiện trong Linear B, song hiếm khi thấy nó xuất hiện ở cuối một từ, điều này cho thấy Linear B không thể là tiếng Hy Lạp. Điều mà mọi người đều nhất trí, đó là Linear B, chữ viết cổ hơn, là đại diện cho một thứ ngôn ngữ còn chưa biết và đã bị mai một. Khi ngôn ngữ này biến mất, chữ viết vẫn còn và tiến hóa qua nhiều thế kỷ thành chữ viết Cypriot, được sử dụng để viết tiếng Hy Lạp. Vì vậy, hai chữ viết trông tương tự nhau nhưng biểu thị hai thứ ngôn ngữ hoàn toàn khác nhau.

Arthur Evans là người ủng hộ tích cực thuyết cho rằng Linear B không phải là dạng chữ viết tiếng Hy Lạp, và ông đinh ninh là nó biểu thị ngôn ngữ Crete bản xứ. Ông tin tưởng rằng có những bằng chứng khảo cổ chắc chắn khẳng định lý lẽ của mình. Chẳng hạn, những khám phá của ông trên đảo Crete cho thấy đế chế của Vua Minoa, còn được biết tới là đế chế Minoa, tiến bộ hơn rất nhiều so với nền văn minh Mycenae trên lục địa. Đế chế Minoa không phải là một lãnh địa của đế chế Mycenae, mà là một thế lực thù địch, thậm chí còn có phần lấn át. Thần thoại về con Nhân Ngưu đã ủng hộ cho quan điểm này. Câu chuyện thần thoại này đã mô tả việc Vua Minoa yêu cầu người Athen cống nạp cho mình các nam thanh nữ tú để hiến tế cho Nhân Ngưu. Nói tóm lại, Evans kết luận rằng người Minoa đã rất thành công khi họ vẫn bảo tồn được tiếng mẹ đẻ của mình, không để cho ngôn ngữ kẻ thù của họ đồng hóa.

Mặc dù việc người Minoa nói thứ ngôn ngữ riêng của họ (và Linear B biểu thị ngôn ngữ này), chứ không phải là tiếng Hy Lạp, đã được chấp nhận rộng rãi song vẫn còn đôi ba người cho rằng người Minoa nói và viết tiếng Hy Lạp. Ngài Arthur không mảy may để tâm đến những ý kiến bất đồng như vậy, và đã sử dụng ảnh hưởng của mình để trừng phạt những người không đồng quan điểm với ông. Khi A. J. B. Wace, giáo sư khảo cổ học của Đại học Cambridge, tuyên bố ủng hộ thuyết cho rằng Linear B biểu thị tiếng Hy Lạp, Ngài Arthur đã loại ông ra khỏi các cuộc khai quật và buộc ông phải về hưu từ trường British School ở Athens.

Hình 58. Một tấm khắc Linear B, 1400 trước Công nguyên

Năm 1939, cuộc tranh luận "Hy Lạp và phi Hy Lạp" lại càng thêm gay gắt khi Carl Blegen của trường Đại học Cincinnati đã tìm thấy một loạt những tấm khắc Linear B ở cung điện Nestor ở Pylos. Điều này quả là khác thường vì Pylos nằm trên lục địa Hy Lạp, và là một vùng thuộc đế chế Mycenae chứ không phải Minoa. Một số ít các nhà khảo cổ vốn tin Linear B là tiếng Hy Lạp cho rằng điều này đã ủng hộ giả thuyết của họ: Linear B được tìm thấy trên lục địa mà ở đó người ta nói tiếng Hy Lạp, và vì vậy Linear B phải biểu thị tiếng Hy Lạp; Linear B cũng được tìm thấy ở Crete, như vậy thì người Minoa cũng nói tiếng Hy Lạp.



Phe Evans tranh luận ngược lại: người Minoa ở Crete nói tiếng Minoa; Linear B được tìm thấy ở Crete, vì vậy Linear B biểu thị ngôn ngữ Minoa; Linear B cũng được tìm thấy ở lục địa vì vậy trên lục địa người ta cũng nói tiếng Minoa. Ngài Arthur nhấn mạnh: "ở Mycenae không có chỗ cho những vị vua nói tiếng Hy Lạp... văn hóa, cũng giống như ngôn ngữ, vẫn còn là Minoa một trăm phần trăm."

Thực tế, khám phá của Blegen không nhất thiết phải áp đặt một ngôn ngữ duy nhất cho người Mycenae và Minoa. Vào thời Trung cổ, rất nhiều nhà nước châu Âu, bất kể nói ngôn ngữ nào, cũng đều ghi chép bằng tiếng Latin. Có thể ngôn ngữ của Linear B cũng là một ngôn ngữ chung của những người làm kế toán ở vùng biển Aege để đơn giản quan hệ buôn bán giữa các quốc gia không cùng nói chung một ngôn ngữ.

Trong vòng bốn thập kỷ, mọi nỗ lực nhằm giải mã Linear B đều kết thúc thất bại. Sau đó, vào năm 1941, Ngài Arthur qua đời ở tuổi 90. Ông đã không còn sống để chứng kiến việc giải mã Linear B, hoặc tự mình đọc được ý nghĩa của những văn bản mà ông đã tìm ra. Thực sự thì vào lúc đó cũng không có nhiều triển vọng là sẽ giải mã được nó.

Các âm tiết nối

Sau cái chết của Ngài Arthur Evans, kho lưu trữ các tấm khắc Linear B và những ghi chép khảo cổ của riêng ông chỉ được một nhóm nhỏ các nhà khảo cổ sử dụng, đó là những người ủng hộ thuyết của ông cho rằng Linear B thể hiện ngôn ngữ riêng của người Minoa. Tuy nhiên, vào giữa những năm 1940,

Alice Kober, một chuyên gia về tiếng Hy Lạp và La Mã cổ ở trường Brooklyn College, đã quyết định tiếp cận các tài liệu này và bắt đầu phân tích chữ viết đó một cách kỹ lưỡng và vô tư. Đối với những người chỉ biết bà một cách sơ sơ thì Kober dường như là một phụ nữ hết sức bình thường - một giáo sư ăn vận xuềnh xoàng, không duyên dáng cũng chẳng lôi cuốn, với lối sống rất giản dị. Tuy nhiên, niềm say mê nghiên cứu của bà thì quả là vô hạn. "Bà làm việc với một cường độ rất cao", Eva Brann, nguyên là một sinh viên theo học ngành khảo cổ của Đại học Yale nhớ lại, "Bà từng nói với tôi rằng chỉ có một cách để biết khi nào mình đã hoàn thành một việc gì đó thực sự to lớn, đó là khi có cảm giác xương sống bị đau ê ẩm".

Alice Kober

Để đột phá Linear B, Kober nhận thấy rằng bà cần phải loại bỏ tất cả mọi định kiến. Bà đã tập trung không vào gì khác ngoài cấu trúc tổng thể của chữ viết và kết cấu của từng từ. Đặc biệt, bà chú ý đến những từ tạo nên các bộ ba, vì chúng dường như là cùng một từ nhưng xuất hiện ở ba dạng hơi khác nhau. Trong một bộ ba từ này, gốc từ là giống nhau, chỉ có ba phần đuôi là khác nhau. Bà kết luận rằng Linear B là thể hiện của một ngôn ngữ biến cách rất cao, tức là đuôi các từ thay đổi để phản ánh

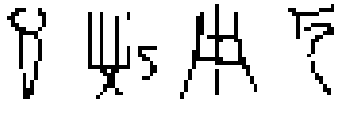
giới tính, thời, cách và những thứ tương tự như vậy. Tiếng Anh là ngôn ngữ biến cách ít vì, chẳng hạn, như chúng ta nói "I decipher, you decipher, he deciphers" *(Tôi giải mã, anh giải mã, anh ấy giải mã)* - ở ngôi thứ ba, động từ có thêm "s". Tuy nhiên, các ngôn ngữ cổ có xu hướng khắt khe và cực đoan hơn rất nhiều trong việc sử dụng vĩ tố (đuôi) của từ. Kober đã công bố một bài báo, trong đó bà mô tả bản chất biến cách của hai nhóm từ cụ thể, như trình bày ở Bảng 17. Mỗi nhóm vẫn giữ nguyên các gốc từ tương ứng của chúng, trong khi đó lại có các đuôi khác nhau tùy theo ba cách khác nhau.

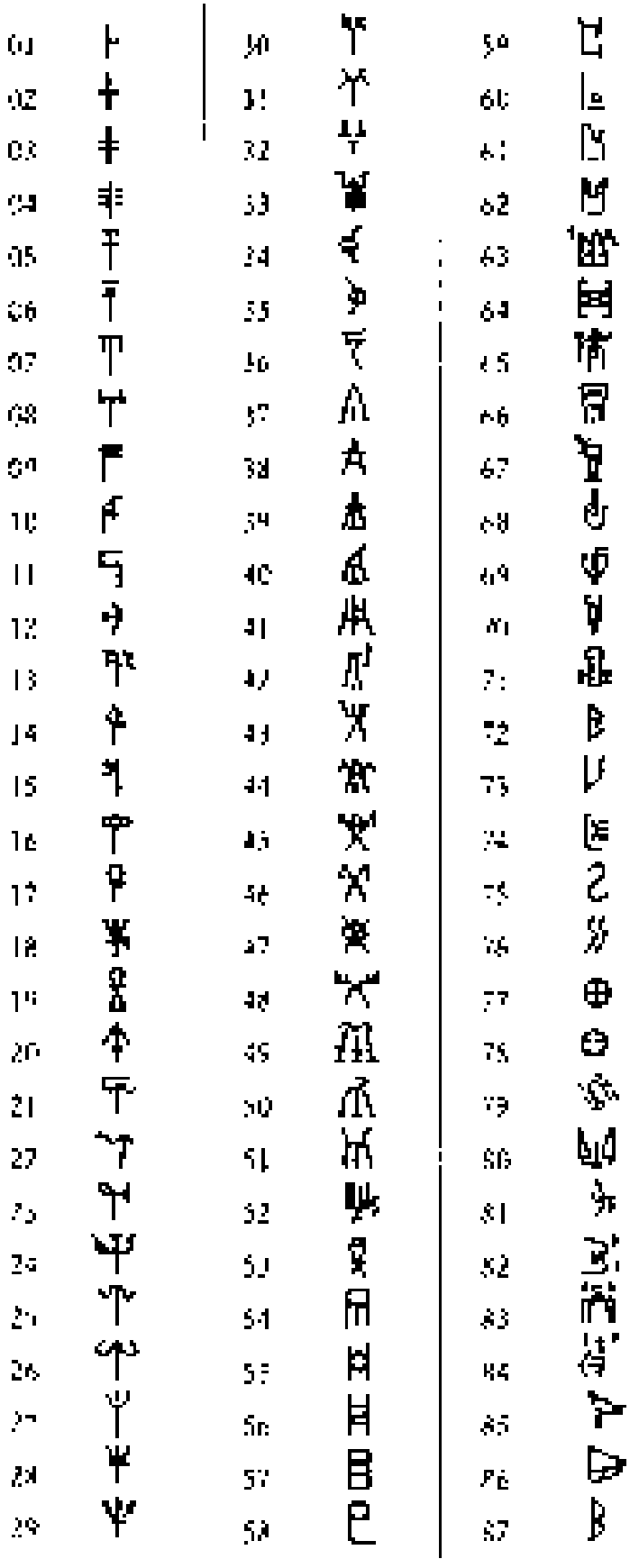
Để dễ thảo luận, mỗi ký hiệu của Linear B được gán cho một số gồm hai chữ số, như trình bày ở Bảng 18. Sử dụng các số này, các từ trong Bảng 17 có thể được viết lại ở Bảng 19. Cả hai nhóm từ này đều có thể là các danh từ có đuôi biến đổi theo các cách - chẳng hạn, trường hợp một có thể là danh cách (chủ ngữ), trường hợp hai là đối cách (bổ ngữ), và trường hợp ba là tặng cách. Rõ ràng là hai ký hiệu đầu tiên trong cả hai nhóm từ (**25-67** và **70-52**) đều là gốc từ, vì chúng được lặp lại ở mọi trường hợp. Tuy nhiên, ký hiệu thứ ba hơi khó hiểu hơn. Nếu ký hiệu thứ ba là một phần của gốc từ thì đối với từ đã cho nó phải không đổi, bất kể là ở cách nào, nhưng đằng này lại không phải như vậy. Ở từ A, ký hiệu thứ ba là **37** trong trường hợp một và hai, nhưng lại là **05** trong trường hợp ba. Ở từ B, ký hiệu thứ ba là **41** trong trường hợp một và hai, nhưng lại là **12** trong trường hợp thứ ba. Một giả thuyết khác, nếu ký hiệu thứ ba không phải là một phần của gốc từ thì có thể nó là phần đuôi của từ, song khả năng này cũng không chắc chắn lắm. Đối với một cách cho trước, thì đuôi từ sẽ phải như nhau bất kể là đuôi từ nào, nhưng ở trường hợp

một và hai, ký hiệu thứ ba là **37** ở từ A, nhưng lại là **41** ở từ B, và trường hợp ba, ký hiệu thứ ba lại là **05** ở từ A và **12** ở từ B.

Ký hiệu thứ ba không tuân theo dự đoán vì chúng dường như không phải là một phần của gốc từ cũng không phải đuôi từ. Kober đã giải quyết nghịch lý này bằng cách viện đến thuyết cho rằng mỗi ký hiệu biểu thị cho một âm tiết, có thể là sự kết hợp của một phụ âm và một nguyên âm tiếp sau. Bà cho rằng âm tiết thứ ba có thể là một âm tiết nối, biểu thị một phần của gốc từ và một phần của đuôi từ. Phụ âm có thể thuộc về gốc từ và nguyên âm là của đuôi từ. Để chứng minh cho giả thuyết này, bà lấy một ví dụ từ ngôn ngữ Akkadian, một ngôn ngữ cũng có các âm tiết nối và cũng có sự biến cách cao. *Sadanu* là danh từ ở cách 1 trong tiếng Akkadian, nó biến đổi thành *sadani* ở cách 2 và thành *sadu* ở cách 3 (Bảng 20). Rõ ràng là ba từ đều chứa gốc từ là **sad**-, và đuôi là -**anu** (cách 1), -**ani** (cách 2), hay -**u** (cách 3), với -**da**, -**da** hay -**du** là các âm tiết nối. Âm tiết nối giống nhau ở cách 1 và 2, song lại khác ở cách 3. Điều này cũng giống hệt như các hình mẫu quan sát thấy trong Linear B - ký hiệu thứ ba trong mỗi từ Linear B của Kober phải là một âm tiết nối.

Bảng 17. Hai từ biến cách trong Linear B

	Từ A	**Từ B**
Trường hợp một		
Trường hợp hai		
Trường hợp ba		



Hình 18. Các ký hiệu Linear B và các con số gán cho chúng.

Chỉ bằng việc xác định được bản chất biến cách của Linear B và sự tồn tại của các âm nối thôi, Kober đã tiến xa hơn bất kỳ ai khác trong việc giải mã các chữ viết Minoa, song điều này mới chỉ là bắt đầu. Bà còn định đưa ra những suy luận thậm chí còn lớn hơn nữa. Trong ví dụ về ngôn ngữ Akkadian, âm tiết nối biến đổi từ *da* sang *du*, song phụ âm lại như nhau ở cả hai âm tiết. Tương tự, âm tiết ở Linear B là **37** và **05** ở từ A sẽ phải có cùng một phụ âm, như các âm tiết **41** và **12** trong từ B. Lần đầu tiên kể từ khi Evans khám phá ra Linear B, sự thực về ngữ âm của các ký tự đã dần bộc lộ. Kober cũng còn xác lập được một tập hợp các mối quan hệ khác giữa các ký tự. Rõ ràng là các từ A và B trong Linear B ở cách 1 có cùng một đuôi. Tuy nhiên, âm nối biến đổi từ **37** thành **41**. Điều này chứng tỏ ký hiệu **37** và **41** biểu thị các âm tiết với các phụ âm khác nhau nhưng nguyên âm thì giống hệt nhau. Điều này lý giải vì sao các ký hiệu là khác nhau trong khi vẫn có đuôi như nhau ở cả hai từ. Tương tự đối với các danh từ ở cách 3, các âm tiết **05** và **12** sẽ có cùng nguyên âm nhưng lại khác phụ âm.

Bảng 19. Hai từ Linear B biến cách được viết lại bằng các con số

	Từ A	**Từ B**
Cách 1	25-67-37-57	70-52-41-57
Cách 2	25-67-37-36	70-52-41-36
Cách 3	25-67-05	70-52-12

Kober không thể chỉ ra được chính xác nguyên âm nào chung cho **05** và **12**, và chung cho **37** và **41**; tương tự bà cũng không xác định được chính xác phụ âm nào chung cho **37** và **05**, và chung cho **41** và **12**. Tuy nhiên, bất kể giá trị ngữ âm đích xác của chúng

là gì thì bà cũng đã thiết lập được mối quan hệ chặt chẽ giữa các ký tự nhất định. Bà đã tổng kết các kết quả của mình trong Bảng 21. Từ Bảng này ta thấy rằng, tuy Kober không biết âm tiết được biểu thị bởi ký hiệu **37**, song bà biết phụ âm của nó được dùng chung với ký hiệu **05** và nguyên âm của nó dùng chung với ký hiệu **41**. Tương tự, bà cũng không biết âm tiết được biểu thị bởi ký hiệu **12**, song bà đã biết phụ âm của nó dùng chung với ký hiệu **41** và nguyên âm của nó dùng chung với ký hiệu **05**. Áp dụng phương pháp của mình với các từ khác, cuối cùng bà đã thiết lập được một bảng gồm 10 ký hiệu, hai cột nguyên âm và năm dòng phụ âm. Lẽ ra Kober hoàn toàn có thể thực hiện được bước đột phá quan trọng tiếp theo và thậm chí có thể giải mã được toàn bộ văn bản. Tuy nhiên, bà đã không sống đủ lâu để khai thác tiếp kết quả công việc của mình. Năm 1950, bà đã mất vì bị ung thư phổi ở tuổi 34.

Bảng 20. Các âm nối trong danh từ *sadanu* của tiếng Akkadian

Cách 1	**sa-da-nu**
Cách 2	**sa-da-ni**
Cách 3	**sa-du**

Một sự lạc hướng vô nghĩa

Chỉ một vài tháng trước khi mất, Alice Kober đã nhận được một bức thư của Michael Ventris, một kiến trúc sư người Anh, người cũng bị Linear B hấp dẫn từ khi ông còn là một đứa trẻ. Ventris sinh ngày 12 tháng Bảy năm 1922, con trai của một quân nhân Anh và người vợ mang nửa dòng máu Ba Lan. Mẹ ông đã có công lớn trong việc khơi dậy trong ông niềm đam mê khảo cổ học.

Bà thường dẫn ông tới Bảo tàng Anh, nơi ông luôn kinh ngạc trước những kỳ quan của thế giới cổ đại. Michael là một cậu bé rất sáng dạ với một năng khiếu kỳ lạ đặc biệt về ngôn ngữ. Khi bắt đầu đi học, cậu đến Gstaad ở Thụy Sĩ và ở đây cậu đã thông thạo tiếng Pháp và tiếng Đức. Sau đó, khi được 6 tuổi, cậu đã tự học tiếng Ba Lan.

Cũng giống như Jean-Franois Champollion, Ventris đã sớm phát triển tình yêu đối với những chữ viết cổ. Khi lên bảy, cậu đã nghiên cứu một cuốn sách về chữ tượng hình Ai Cập, một thành tích đầy ấn tượng ở lứa tuổi bé như vậy, nhất là khi cuốn sách lại được viết bằng tiếng Đức. Sự hứng thú đối với chữ viết của các nền văn minh cổ này vẫn tiếp tục duy trì trong suốt thời niên thiếu của ông. Năm 1936, ở tuổi 14, niềm đam mê này lại được thổi bùng lên thêm khi ông tham dự buổi thuyết trình của Ngài Arthur Evans, người đã phám phá ra Linear B. Chàng trai trẻ Ventris đã nghiên cứu về nền văn minh Minoa và bí ẩn của các bản khắc Linear B, và tự hứa với mình là sẽ giải mã bằng được nó. Chính từ ngày đó, một nỗi ám ảnh nảy sinh và đeo bám theo Ventris suốt cuộc đời tuy ngắn ngủi nhưng sáng chói của ông.

Bảng 21 Hệ thống của Kober biểu thị mối quan hệ giữa các ký tự Linear B

	Nguyên âm I	Nguyên âm II
Phụ âm I	37	05
Phụ âm II	41	12

Khi mới 18 tuổi, ông đã tóm tắt lại những ý tưởng ban đầu về Linear B trong một bài báo được công bố sau đó trên tạp chí danh tiếng *American Journal of Archaeology* (Tạp chí Khảo

Michael Ventris

cổ học của Mỹ). Khi gửi bài báo, ông đã rất thận trọng giấu các biên tập viên của tạp chí tuổi của mình vì sợ không được xem trọng. Bài báo của ông đã ủng hộ rất mạnh mẽ những chỉ trích của Ngài Arthur đối với thuyết ngôn ngữ Hy Lạp, trong đó ông khẳng định: "Thuyết cho rằng tiếng của người Minoa có thể là tiếng Hy Lạp tất nhiên là dựa trên sự thiếu suy xét một cách thận trọng đến tính hợp lý lịch sử". Bản thân ông tin rằng Linear B có liên quan đến tiếng Etrusca. Đây là một quan điểm hợp lý vì có bằng chứng cho thấy người Etrusca đã đến từ Aege trước khi định cư tại Italia. Mặc dù bài báo của ông không nhằm vào việc giải mã song ông kết luận một cách tự tin rằng: "Việc đó có thể sẽ làm được".

Nhưng rồi Ventris trở thành một kiến trúc sư chứ không phải một nhà khảo cổ học chuyên nghiệp, song niềm đam mê Linear B vẫn không hề phai nhạt nên ông dành hết thời gian rảnh rỗi để nghiên cứu mọi khía cạnh của thứ chữ viết này. Khi nghe tin về công trình của Alice Kober, ông đã rất sốt sắng tìm hiểu các thành quả của bà, và thậm chí ông còn viết thư cho bà để hỏi cụ thể hơn. Mặc dù bà đã qua đời trước khi trả lời ông, song những ý tưởng của bà vẫn sống mãi trong các công trình đã được công

bố và Ventris đã nghiên cứu chúng một cách rất kỹ lưỡng. Ông đánh giá cao tầm quan trọng của hệ thống các bảng của Kober và cố gắng tìm thêm các từ mới có chung gốc từ và các âm tiết nối. Ông đã mở rộng thêm hệ thống các bảng của bà bằng các ký hiệu mới này, bao gồm các nguyên âm và phụ âm khác. Sau một năm miệt mài nghiên cứu, ông đã nhận thấy một điều gì đó thật đặc biệt, nó dường như gợi ý về một ngoại lệ của quy tắc cho rằng tất cả các ký hiệu trong Linear B đều là các âm tiết.

Nói chung, dường như mọi người giờ đây đều đã nhất trí rằng mỗi ký hiệu của Linear B là sự kết hợp của một phụ âm với một nguyên âm (CV), và vì vậy khi đánh vần sẽ phải chia một từ thành các thành phần CV. Ví dụ, từ **minute** trong tiếng Anh, sẽ được đánh vần là **mi-nu-te**, một tập hợp gồm ba âm tiết CV. Tuy nhiên, có nhiều từ không thể phân chia thành các âm tiết CV được. Ví dụ, nếu chúng ta chia từ "visible" thành các cặp chữ cái, chúng ta sẽ được **vi-si-bl-e**, như vậy thì xem ra không ổn, vì nó không bao gồm một dãy chỉ gồm các cặp âm tiết CV: ở đây có một âm tiết hai phụ âm và thừa chữ **e** ở đuôi từ. Ventris cho rằng người Minoa khắc phục vấn đề này bằng cách chèn vào một âm **i** câm tạo ra âm tiết làm đẹp **-bi-**, nên từ này giờ sẽ được viết thành **vi-si-bi-le**, đúng là một sự kết hợp của các âm tiết CV.

Tuy nhiên, đối với từ **invisible** thì lại có vấn đề. Một lần nữa lại cần phải chèn vào các nguyên âm câm, lần này là sau **n** và sau **b**, để chuyển chúng thành các âm tiết CV. Hơn nữa, còn phải giải quyết cả nguyên âm **i** ở đầu từ: **i-ni-vi-si-bi-le**. Chữ cái đầu **i** không thể dễ dàng chuyển thành âm tiết CV, vì nếu thêm phụ âm câm vào đầu từ có thể sẽ dễ gây ra nhầm lẫn. Tóm lại, Ventris kết luận rằng phải có những ký hiệu Linear B biểu thị cho những nguyên

Bảng 22. Bảng mở rộng của Ventris về các mối quan hệ giữa các ký tự trong Linear B. Mặc dù bảng không xác định rõ các nguyên âm hay phụ âm, song nó đã nêu bật được ký tự nào cùng có chung nguyên âm và phụ âm. Chẳng hạn, tất cả các ký tự trong cột đầu tiên có chung nguyên âm, được đánh số 1.

Phụ âm	Nguyên âm				
	1	2	3	4	5
I					57
II	40		75		54
III	30				03
IV		16			
V		14			01
VI	37	05		69	
VII	41	17			31
VIII	30	52	24	55	06
IX	73	15			80
X		70	44		
XI	91				76
XII		02	27		
XIII					
XIV			14		
XV		32	70		
Thuần nguyên âm		61			08

âm đơn, được sử dụng trong các từ bắt đầu bằng một nguyên âm. Các ký hiệu này dễ phát hiện vì chúng chỉ xuất hiện ở đầu các từ. Ventris đã tính toán xác suất từng ký hiệu xuất hiện ở đầu từ, giữa từ và cuối từ. Ông quan sát thấy hai ký hiệu đặc biệt, là **08** và **61**, phần lớn được tìm thấy ở đầu từ, và kết luận rằng chúng không biểu thị cho âm tiết mà là các nguyên âm đơn.

Ventris đã công bố các ý tưởng của mình về các ký hiệu nguyên âm và sự mở rộng hệ thống bảng của Kober trong loạt sách *Work Notes* (Ghi chép làm việc) và gửi chúng cho các nhà nghiên cứu

Linear B khác. Vào ngày 1 tháng Sáu năm 1952, ông đã công bố kết quả quan trọng nhất của mình trong *Work Note* số 20, một bước ngoặt trong việc giải mã Linear B. Ông đã dành hai năm cuối đời để mở rộng thêm hệ thống bảng của Kober như trình bày ở Bảng 22. Bảng gồm năm cột nguyên âm và 15 hàng phụ âm, tổng cộng là 75 ô, với 5 ô phụ thêm cho các nguyên âm đơn. Ventris đã điền các ký hiệu vào khoảng một nửa số ô. Bảng này là một kho thông tin quý báu. Chẳng hạn, từ hàng thứ 6, có thể nói ký hiệu âm tiết **37**, **05** và **69** cùng có chung một phụ âm, VI, song lại có nguyên âm khác nhau là 1, 2 và 4. Ventris không biết giá trị chính xác của phụ âm VI hay các nguyên âm 1, 2, và 4, và đến lúc này, ông vẫn cưỡng lại được sự cám dỗ của việc gán các giá trị âm cho các ký hiệu đó. Tuy nhiên, ông cảm thấy rằng đây chính là lúc để nghe theo một số linh cảm, dự đoán một vài giá trị âm và kiểm định các hệ quả rút ra từ đó.

Ventris chú ý đến ba từ xuất hiện lặp đi lặp lại trên một số tấm Linear B: **08-73-30-12**, **70-52-12** và **69-53-12**. Chỉ dựa trên trực giác, ông đoán rằng các từ này có thể là tên của các thị trấn quan trọng. Ventris đã suy đoán rằng ký hiệu **08** là một nguyên âm và vì vậy tên của thị trấn đầu tiên phải được bắt đầu bằng một nguyên âm. Chỉ có một cái tên quan trọng phù hợp với yêu cầu này là Amnisos, một hải cảng quan trọng. Nếu ông đúng thì ký hiệu thứ hai và thứ ba, **73** và **30**, sẽ biểu thị các âm **-mi-** và **-ni-**. Hai âm tiết này đều có chứa cùng một nguyên âm là **i**, như vậy thì **73** và **30** phải ở cùng một cột nguyên âm trong bảng. Quả đúng là như vậy. Ký hiệu cuối cùng, **12**, biểu thị âm **-so-**, và như vậy không còn ký hiệu nào biểu thị âm **s**. Ventris quyết định tạm thời bỏ qua chuyện âm s này và đi đến kết quả dịch như sau:

Thị trấn 1 = **08-30-12** = **a-mi-ni-so** = Amnisos

Đây chỉ là phỏng đoán, song ảnh hưởng của nó đến bảng của Ventris là rất lớn. Chẳng hạn, ký hiệu **12**, có thể biểu thị cho **-so-**, thuộc cột nguyên âm số 2 và hàng phụ âm số 7. Vì vậy, nếu dự đoán của ông chính xác thì tất cả các ký hiệu âm tiết khác trong cột nguyên âm thứ 2 sẽ có chứa nguyên âm **o**, và tất cả các ký hiệu âm tiết trong hàng phụ âm thứ 7 sẽ có chứa phụ âm **s**.

Khi Ventris xem xét đến thị trấn thứ 2, ông nhận thấy rằng nó cũng có chứa ký hiệu **12**, tức âm tiết **-so-**. Các ký hiệu khác là **70** và **52**, đều cùng trong cột nguyên âm như **-so-**, tức là các ký hiệu này cũng có chứa nguyên âm **o**. Đối với thị trấn thứ 2, ông có thể điền **-so-** và **o** vào các vị trí thích hợp và để lại những chỗ trống của các phụ âm chưa biết, và thu được kết quả sau:

Thị trấn 2 = **70-52-12** =**?o-?o-so** =?

Liệu nó có phải là Knossos? Các ký hiệu có thể biểu thị **ko-no-so**. Một lần nữa, Ventris lại vui vẻ bỏ qua vấn đề thiếu chữ cái cuối cùng **s**, ít nhất là vào lúc này. Ông hài lòng nhận thấy rằng ký hiệu **52**, giả định là biểu thị **-no-**, ở cùng một hàng phụ âm với ký hiệu **30**, giả định là biểu thị **-ni-** trong Amnisos. Điều này là chắc chắn vì nếu chúng có chung phụ âm **n** thì chúng phải thực sự ở trên cùng một hàng phụ âm. Sử dụng thông tin từ các âm tiết của Knossos và Amnisos, ông điền các chữ cái vào tên thị trấn thứ 3:

Thị trấn 3 = **69-53-12=??-?i-so**

Chỉ có một cái tên có vẻ thích hợp là Tulissos (**tu-li-so**), một thị trấn quan trọng nằm ở trung tâm Crete. Một lần nữa, chữ cái cuối cùng **s** lại bị thiếu và một lần nữa Ventris lại tạm lờ đi vấn

đề này. Giờ thì ông đã xác định được ba địa danh và giá trị âm tiết của tám ký hiệu khác nhau:

Thị trấn 1 = **08-73-30-12**	**=a-mi-ni-so**	= Amnisos
Thị trấn 2 = **70-52-12**	**=ko-no-so**	= Knossos
Thị trấn 3 = **69-53-12**	**=tu-li-so**	= Tulissos

Việc xác định được tám ký hiệu này có ý nghĩa rất lớn. Từ đây Ventris có thể suy ra các giá trị phụ âm và nguyên âm của các ký hiệu khác trong bảng, nếu chúng ở trên cùng một hàng hoặc một cột. Kết quả là rất nhiều ký hiệu đã tiết lộ một phần ý nghĩa âm tiết của chúng và một số có thể được xác định đầy đủ. Chẳng hạn, ký hiệu **05** trong cùng một cột với **12 (so)**, **52 (no)** và **70 (ko)** và vì vậy phải chứa nguyên âm **o**. Bằng quá trình lập luận tương tự, ký hiệu **05** ở cùng một hàng với **69 (tu)**, và vì vậy có chứa phụ âm **t**. Kết quả, ký hiệu **05** biểu thị cho âm tiết **-to-**. Đến ký hiệu **31**, nó ở cùng một cột với ký hiệu **08**, cột **a**, và cùng hàng với ký hiệu **12**, hàng **s**. Vì vậy ký hiệu **31** biểu thị cho âm tiết **-sa-**.

Việc suy ra các giá trị âm tiết của hai ký hiệu **05** và **31** là đặc biệt quan trọng vì nó cho phép Ventris đọc được hai từ trọn vẹn, đó là **05-12** và **05-31**, thường xuất hiện ở cuối các bản kiểm kê. Ventris đã biết ký hiệu **12** biểu thị cho âm tiết **-so-**, vì ký hiệu này xuất hiện trong từ Tulissos, và do vậy **05-12** có thể được đọc là **to-so**. Và từ còn lại, **05-31**, có thể được đọc là **to-sa**. Đây quả là một kết quả đáng kinh ngạc. Vì các từ này luôn xuất hiện ở cuối các bản kiểm kê, nên các chuyên gia cho rằng chúng có nghĩa là "total" *(tổng cộng* - ND). Lúc này Ventris đọc chúng là **toso** và **tosa**, giống một cách kỳ lạ với các từ *tossos* và *tossa* trong tiếng

Hy Lạp cổ, là dạng giống đực và giống cái của từ có nghĩa là "rất nhiều". Ngay hồi mới 14 tuổi, từ thời điểm được nghe Ngài Arthur Evans nói chuyện, ông đã tin rằng ngôn ngữ của người Minoa không thể là tiếng Hy Lạp. Nhưng giờ đây ông lại khám phá ra các từ là bằng chứng rõ ràng ủng hộ cho quan điểm coi tiếng Hy Lạp là ngôn ngữ của Linear B.

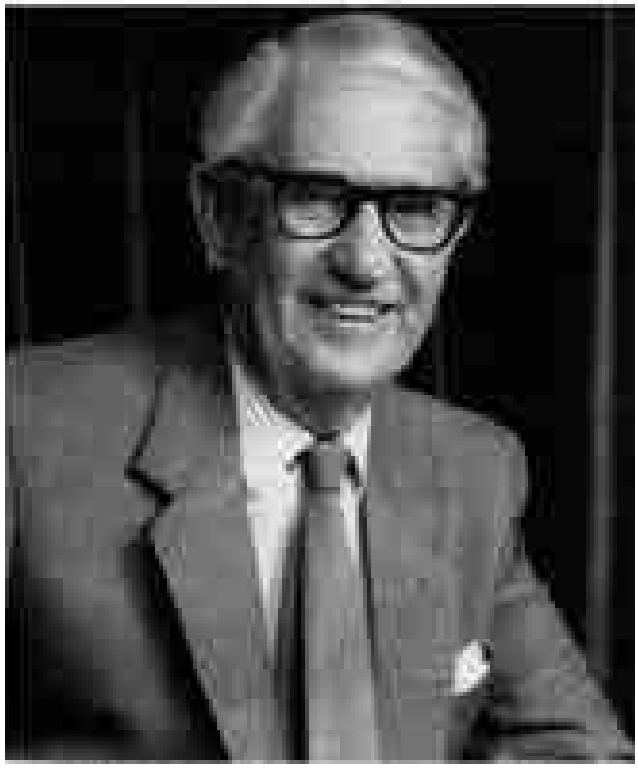
Chính văn tự Cypriot cổ đã cung cấp một số bằng chứng sớm nhất chống lại quan điểm xem Linear B là tiếng Hy Lạp, vì nó gợi ý rằng các từ của Linear B ít khi có đuôi là **s**, trong khi đó đuôi này lại rất thông dụng trong tiếng Hy Lạp. Ventris đã khám phá ra rằng thực sự thì các từ trong Linear B hiếm khi có đuôi **s**, song có thể điều này chỉ đơn giản là vì việc bỏ **s** đi là một phần trong quy ước viết nào đó. Aminisos, Knossos, Tulissos và *tossos* đều được đánh vần thiếu chữ **s** ở cuối, cho thấy người viết đơn giản là không hề quan tâm đến chữ **s**, để người đọc tự điền vào sự thiếu hụt hiển nhiên này.

Chẳng bao lâu sau, Ventris đã giải mã được một số từ khác, cũng có liên quan đến tiếng Hy Lạp, song ông vẫn hoàn toàn chưa tin chắc Linear B là chữ viết tiếng Hy Lạp. Về lý thuyết, một số từ mà ông giải mã được đều có thể coi như những từ vay mượn trong ngôn ngữ Minoa. Một người nước ngoài đến một khách sạn ở Anh có thể nghe thấy một số từ như "rendez-vous" hay "bon appetit", song sẽ là sai lầm nếu cho rằng người Anh nói tiếng Pháp. Hơn nữa, Ventris cũng đã gặp các từ không có ý nghĩa gì đối với ông, điều này lại cung cấp bằng chứng nữa ủng hộ cho thứ ngôn ngữ còn chưa biết cho tới lúc đó. Trong *Work Note 20,* ông không hoàn toàn chối bỏ thuyết tiếng Hy Lạp song ông gọi đó là "một sự lạc hướng vô nghĩa". Ông kết

luận: "Nếu tiếp tục theo đuổi thì tôi ngờ rằng hướng giải mã này không sớm thì muộn cũng sẽ đi đến bế tắc, hoặc tự nó tiêu tan vì phi lý".

Mặc cho sự nghi ngại đó, Ventris vẫn theo đuổi hướng tiếng Hy Lạp. Trong khi *Work Note 20* còn đang được phát hành thì ông đã khám phá được thêm nhiều từ Hy Lạp nữa. Ông đã xác định được từ *poimen* (người chăn cừu), *kerameus* (thợ gốm), *khrusoworgos* (thợ kim hoàn) và *khalkeus* (thợ đúc đồng), và ông thậm chí còn dịch được cả một số cụm từ hoàn chỉnh. Đến lúc này thì không có sự phi lý đáng sợ nào chặn đường đi của ông nữa. Đây là lần đầu tiên trong ba ngàn năm, chữ viết câm lặng của Linear B lại thì thầm lên tiếng một lần nữa, và ngôn ngữ mà nó nói không nghi ngờ gì nữa chính là tiếng Hy Lạp.

Trong quá trình giải mã nhanh chóng này, Ventris tình cờ được mời phỏng vấn trên đài BBC để thảo luận về bí ẩn chữ viết của người Minoa. Ông quyết định đây là một cơ hội lý tưởng để công bố những khám phá của mình. Sau một hồi thảo luận tẻ ngắt về lịch sử của Minoa và Linear B, ông đã đưa ra một tuyên bố có tính cách mạng của mình: "Trong suốt mấy tuần vừa qua, tôi đã đi đến kết luận rằng các bản khắc đất sét ở Knossos và Pylos, rốt cuộc, phải được viết bằng tiếng Hy Lạp - một thứ tiếng Hy Lạp khó và cổ xưa, bởi vì nó có trước thời Homer tới 500 năm và được viết ở dạng khá tắt, song dù sao thì vẫn là tiếng Hy Lạp". Một trong các thính giả của buổi phát thanh đó là John Chadwick, nhà nghiên cứu thuộc Đại học Cambridge, người đã rất quan tâm đến việc giải mã Linear B từ những năm 1930. Trong chiến tranh, ông từng là nhà giải mã ở Alexandria, nơi ông đã phá được mật mã của người Italia, trước khi chuyển đến



John Chadwick

Bletchley Park, nơi ông đã giải được mật mã của người Nhật Bản. Sau chiến tranh, một lần nữa ông lại thử giải mã Linear B, nhưng lần này ông sử dụng những kỹ thuật mà ông đã học được trong thời gian làm việc với mật mã quân sự. Tiếc thay, ông mới chỉ đạt được chút ít thành công.

Khi nghe được cuộc phỏng vấn trên đài, ông hoàn toàn sửng sốt trước tuyên bố xem ra là hết sức phi lý của Ventris. Chadwick, cùng với phần lớn các học giả nghe đài phát thanh hôm đó, đều bác bỏ tuyên bố này, coi đó là công trình của một tay nghiệp dư - mà thực sự thì cũng đúng là như vậy. Tuy nhiên, là một giảng viên tiếng Hy Lạp, Chadwick nhận ra rằng ông có thể đặt ra hàng loạt câu hỏi liên quan đến tuyên bố của Ventris và để chuẩn bị tấn công, ông quyết định nghiên cứu kỹ lưỡng những lập luận của Ventris. Ông nhận được các *Work Notes* của Ventris và xem xét chúng với hy vọng sẽ tìm thấy ở đó đầy rẫy những lỗ hổng. Tuy nhiên, chỉ trong vài ngày, nhà học giả vốn hoài nghi giờ trở thành một trong những người đầu tiên ủng hộ cho thuyết Hy Lạp về Linear B của Ventris. Chadwick nhanh chóng trở nên ngưỡng mộ nhà kiến trúc sư trẻ tuổi này:

Bộ não của ông (tức Ventris) làm việc với một tốc độ đáng kinh ngạc, nhờ vậy mà ông có thể nghĩ ra tất cả những hàm ý của một đề nghị gần như trước khi bạn nói ra lời. Ông có một sự đánh giá sắc bén về những thực tại của tình thế; những người Mycenae đối với ông không phải là những con người trừu tượng mơ hồ mà là những con người sống động, mà ông có thể nhìn thấu ý nghĩ của họ. Bản thân ông chủ yếu dựa trên sự tiếp cận thị giác đối với vấn đề; ông làm cho mình quen thuộc với khía cạnh thị giác của các văn bản đến nỗi những đoạn dài in sâu trong tâm trí ông một cách đơn giản như là những hình mẫu thị giác từ rất lâu trước khi giải mã ra ý nghĩa của chúng. Song chỉ một trí nhớ như chụp ảnh là chưa đủ, mà ở đây sự đào tạo về kiến trúc đã hỗ trợ ông rất nhiều. Con mắt của nhà kiến trúc sư không chỉ nhìn thấy vẻ ngoài của tòa nhà mà còn cả mớ bòng bong những đặc điểm về trang trí và cấu trúc: nó nhìn vào bên dưới vẻ bề ngoài và phân biệt những bộ phận quan trọng của hình mẫu, các yếu tố cấu trúc và khung sườn của tòa nhà. Vì vậy mà Ventris cũng có thể phân biệt được những hình mẫu và sự cân đối làm lộ ra cấu trúc bên dưới giữa sự đa dạng phức tạp dễ gây bối rối của những ký hiệu bí ẩn. Chính phẩm chất đó, tức năng lực nhìn thấu trật tự bên trong sự hỗn độn bề ngoài, là dấu hiệu nổi bật của tất cả những con người vĩ đại.

Tuy nhiên, Ventris lại thiếu một kỹ năng đặc biệt, đó là kiến thức thấu đáo về tiếng Hy Lạp cổ. Ventris chỉ được học chính quy về tiếng Hy Lạp khi còn là học sinh của trường Stowe, vì vậy ông không thể tận dụng triệt để thành quả của mình. Chẳng hạn, ông không thể giải thích được một số từ đã được giải mã vì chúng không có trong vốn từ vựng tiếng Hy Lạp của ông. Chuyên môn của Chadwick là triết học Hy Lạp, là nghiên cứu sự tiến hóa của

ngôn ngữ Hy Lạp trong lịch sử và vì vậy mà ông được trang bị tốt để chứng minh được những từ còn có vấn đề đó thực ra là hoàn toàn phù hợp với các thuyết về những hình thái cổ nhất của ngôn ngữ Hy Lạp. Chadwick và Ventris cùng với nhau tạo nên một cặp đối tác thật hoàn hảo.

Tiếng Hy Lạp của Homer đã tồn tại cách đây 3000 năm song tiếng Hy Lạp của Linear B còn cổ xưa hơn đến 500 năm. Để dịch được nó, Chadwick cần phải xuất phát từ tiếng Hy Lạp cổ đã được xác lập để ngoại suy ra các từ của Linear B, khi tính đến ba cách phát triển của ngôn ngữ. Thứ nhất, phát âm cũng tiến triển theo thời gian. Ví dụ, từ "vòi tắm" trong tiếng Hy Lạp thay đổi từ *lewotrokhowoi* trong Linear B thành *loutrokhooi* vào thời của Homer. Thứ hai, có sự thay đổi trong ngữ pháp. Ví dụ, trong Linear B sở hữu cách có đuôi là *-oio*, song trong tiếng Hy Lạp cổ thì lại được thay bằng *-ou*. Và cuối cùng, từ vựng cũng có thể thay đổi một cách ghê gớm. Một số từ mới sinh ra, một số mất đi, số khác thì thay đổi nghĩa của chúng. Trong Linear B, *harmo* có nghĩa là "bánh xe" (wheel), song trong tiếng Hy Lạp sau này cũng từ đó lại có nghĩa là "xe ngựa". Chadwick đã chỉ ra điều tương tự đối với việc sử dụng từ "wheels" trong tiếng Anh hiện đại có nghĩa là xe hơi.

Với kỹ năng giải mã của Ventris và chuyên môn tiếng Hy Lạp của Chadwick, cả hai đã thuyết phục được cả thế giới rằng Linear B thực sự là tiếng Hy Lạp. Tốc độ dịch tăng lên mỗi ngày. Trong báo cáo của Chadwick về công việc của họ, *Giải mã Linear B*, ông viết:

> Khoa học mật mã là một môn khoa học của suy luận và thử nghiệm; giả thuyết được đưa ra, kiểm chứng và thường bị loại

bỏ. Song phần còn lại vượt qua được sự kiểm chứng sẽ phát triển cho đến khi, cuối cùng, người thử nghiệm cảm thấy nền đất cứng dưới chân mình: giả thuyết của anh ta là chặt chẽ, và những mảnh vụn ý nghĩa ẩn dưới lớp ngụy trang giờ đột ngột lộ diện. Mật mã "đã bị phá vỡ". Có lẽ điều này được định nghĩa đạt nhất như là thời điểm khi mà sự dẫn dắt đáng tin cậy dường như còn nhanh hơn cả khả năng theo kịp của họ. Nó cũng giống như sự khởi phát một phản ứng dây chuyền trong vật lý hạt nhân; một khi vượt qua ngưỡng tới hạn thì phản ứng sẽ tự nó lan truyền.

Không lâu sau, họ đã chứng minh sự thành thạo của mình về thứ chữ viết này bằng cách viết cho nhau những đoạn thư ngắn bằng chữ viết trong Linear B.

Một cách kiểm tra không chính thức về độ chính xác của một bản giải mã đó là số lượng các vị thần trong văn bản. Ngày trước, những người đi sai hướng, không có gì đáng ngạc nhiên, đã tạo ra những từ vô nghĩa, và chúng thường được giải thích là tên của những vị thần chưa bao giờ được biết tới từ trước đến nay. Tuy nhiên, Chadwick và Ventris có được tên của bốn vị thần, tất cả đều là các vị thần đã biết.

Vào năm 1953, tự tin vào sự giải mã của mình, họ đã công bố thành quả nghiên cứu của mình trong một bài báo có nhan đề khiêm tốn là "Bằng chứng về phương ngữ Hy Lạp trong các lưu trữ của người Mycenae", được đăng trên tạp chí *The Journal of Hellenic Studies* (Tạp chí nghiên cứu tiền văn minh Hy Lạp). Sau đó, các nhà khảo cổ học trên khắp thế giới bắt đầu nhận ra rằng họ đang chứng kiến một cuộc cách mạng. Trong một bức thư gửi Ventris, học giả người Đức, Ernst Sittig đã tóm tắt lại cảm xúc của giới khoa học như sau: "Tôi xin nhắc lại: những chứng minh

của ngài là điều hay nhất về khoa học mật mã mà tôi đã từng được nghe; và nó thực sự là rất hấp dẫn. Nếu các ngài đúng thì các phương pháp khảo cổ học, dân tộc học, lịch sử và triết học của 50 năm gần đây sẽ chỉ còn là những thứ ngớ ngẩn".

Các bản khắc Linear B đã phủ nhận tất cả những tuyên bố của Ngài Arthur Evans và các thế hệ tiếp nối ông. Trước hết, một thực tế đơn giản là Linear B là tiếng Hy Lạp. Thứ hai, nếu người Minoa trên đảo Crete viết tiếng Hy Lạp và có lẽ là nói tiếng Hy Lạp, thì điều này sẽ buộc các nhà khảo cổ học phải xem xét lại quan điểm của họ về lịch sử Minoa. Giờ đây, dường như thế lực thống trị trên khu vực này lại là Mycenae, và Crete của người Minoa, những người phải nói thứ tiếng của những người láng giềng mạnh hơn họ, lại là quốc gia yếu thế hơn. Tuy nhiên, có bằng chứng cho thấy trước năm 1450 trước Công nguyên, Minoa thực sự là một lãnh thổ độc lập với ngôn ngữ riêng của họ. Vào khoảng năm 1450 trước Công nguyên, Linear B đã thay thế Linear A, mặc dù hai dạng chữ viết này trông rất giống nhau, song vẫn chưa có ai giải mã được Linear A. Vì vậy, Linear A có thể đại diện cho một ngôn ngữ hoàn toàn khác biệt với Linear B. Có vẻ như vào khoảng năm 1450 trước Công nguyên, người Mycenae đã chinh phục được Minoa, áp đặt ngôn ngữ của họ và biến đổi Linear A thành Linear B, để nó thực hiện chức năng như một dạng chữ viết của tiếng Hy Lạp.

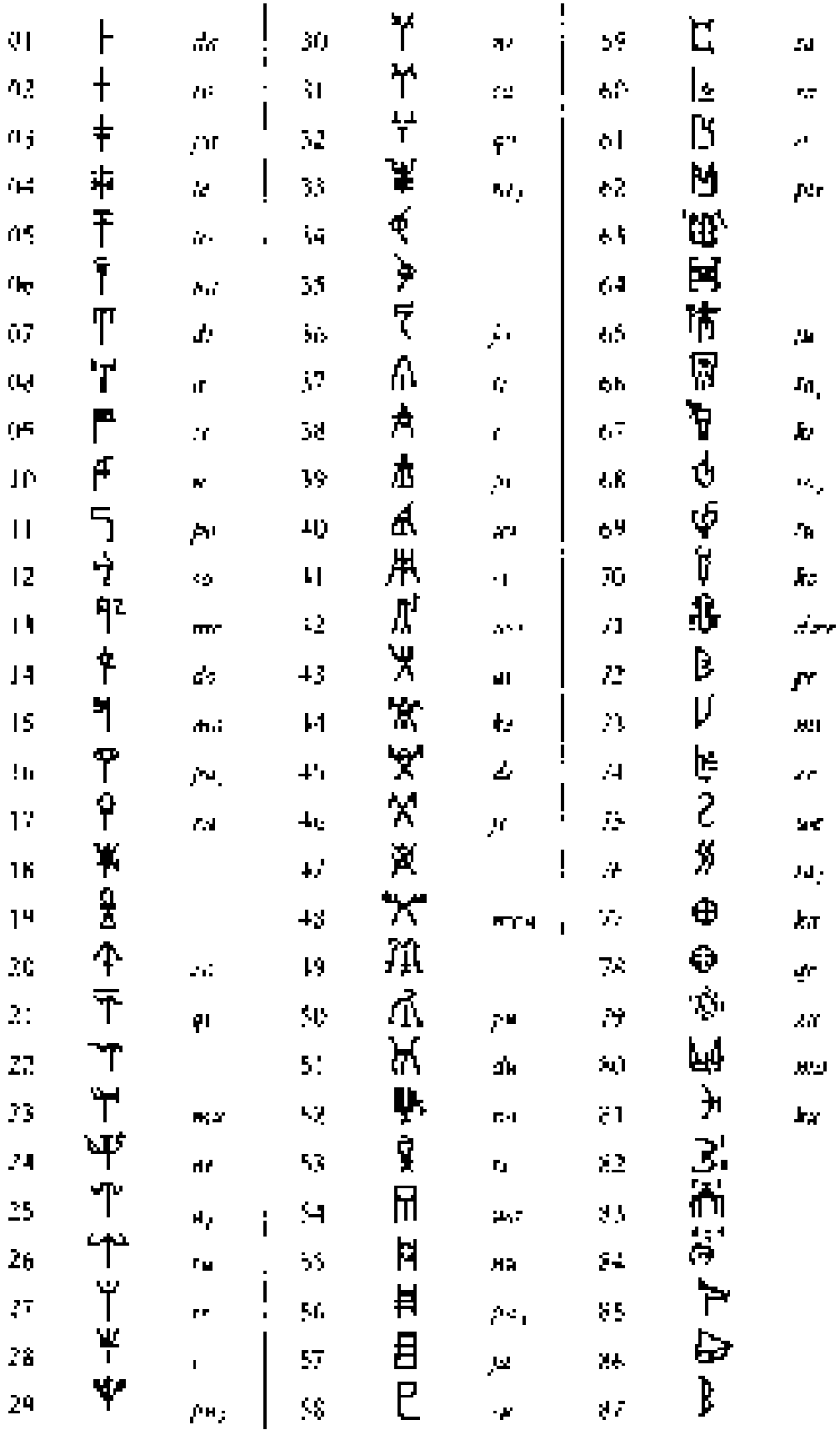
Cùng với việc làm rõ thêm bức tranh lịch sử rộng lớn, việc giải mã Linear B còn bổ sung thêm một số chi tiết. Ví dụ như các cuộc khai quật ở Pylos đã không khám phá ra bất kỳ đồ vật quý giá nào trong cung điện xa hoa, cuối cùng đã bị lửa thiêu hủy. Điều này khiến người ta ngờ rằng cung điện này đã bị cố ý đốt cháy bởi những kẻ tấn công sau khi đã lấy sạch đi những thứ có

giá trị. Mặc dù các tấm Linear B ở Pylos không mô tả một cách cụ thể cuộc tấn công nào như vậy, song họ có bóng gió nói đến sự chuẩn bị cho một cuộc xâm lược. Một tấm mô tả việc thành lập một đội quân đặc biệt để bảo vệ bờ biển, một tấm khác mô tả việc trưng dụng các đồ trang sức bằng đồng để chế tạo đầu giáo mác. Tấm thứ ba, nguệch ngoạc hơn so với hai tấm kia, mô tả việc sửa soạn cụ thể cho nghi lễ đền thờ, có thể có liên quan đến cả việc hiến tế con người. Hầu hết các tấm Linear B đều được xếp đặt ngăn nắp, cho thấy người viết bắt đầu với một bản nháp thô rồi sau đó sẽ hủy đi. Tấm viết nguệch ngoạc có những khoảng trống lớn, những dòng bỏ trống một nửa và chữ viết tràn cả sang mặt bên kia. Một sự giải thích hợp lý đó là tấm này ghi lại lời cầu khẩn thánh thần ngăn chặn cuộc xâm lược, song trước khi tấm này được chép lại thì cung điện đã bị tàn phá.

Phần lớn các tấm Linear B đều là các bảng kiểm kê, và mô tả những giao dịch hằng ngày. Chúng cho thấy sự tồn tại của một bộ máy hành chính chẳng thua kém bộ máy hành chính nào trong lịch sử, với những bản khắc ghi chép chi tiết các hàng hóa sản xuất ra và các sản phẩm nông nghiệp. Chadwick đã ví kho lưu trữ các bản khắc này như cuốn *Domesday Book* (sổ điền thổ lập theo lệnh của William the Conqueror năm 1806, nước Anh - ND), và giáo sư Denys Page đã mô tả ở mức độ chi tiết hơn như sau: "Cừu được đếm đến tổng số ngất ngưởng là hai mươi lăm ngàn con, song người ta cũng không quên ghi lại một thực tế là có ông Komawens nào đó đóng góp chỉ *một* con... Người ta cho rằng không có hạt nào được gieo, không một gam đồng nào được chế tác, không một bộ áo quần nào được may, không một con dê nào được nuôi hay con lợn nào được vỗ béo mà không được điền vào một biểu mẫu

trong Cung điện Hoàng gia." Các ghi chép ở cung điện này có thể dường như là rất trần tục song chúng vốn cũng rất lãng mạn vì có liên quan một cách mật thiết đến các tác phẩm *Odyssey* và *Iliad*. Trong lúc những viên thư lại ở Knossos và Pylos ghi lại những giao dịch hằng ngày của họ thì Cuộc chiến thành Troy khởi tranh. Ngôn ngữ của Linear B chính là ngôn ngữ của Odysseus.

Ngày 24 tháng Sáu năm 1953, Ventris đã có một bài phát biểu trước công chúng tóm tắt việc giải mã Linear B. Ngày sau đó nó đã được đăng lại trên tờ *The Times*, ngay cạnh một bài bình luận về cuộc chinh phục mới nhất đỉnh Everest. Điều này đã khiến cho thành công của Ventris và Chadwick được biết đến như là một "đỉnh Everest trong Khảo cổ học Hy Lạp". Năm sau, hai người quyết định viết một báo cáo gồm ba tập mô tả về công việc của họ, trong đó trình bày việc giải mã, một phân tích chi tiết về ba trăm bản khắc, một từ điển gồm 630 từ Mycenae và một danh sách các giá trị âm của hầu như tất cả các ký hiệu trong Linear B, như trình bày ở Bảng 23. Cuốn *Các tài liệu về tiếng Hy Lạp của người Mycenae* được hoàn tất vào mùa hè năm 1955 và đã sẵn sàng cho việc xuất bản vào mùa thu năm 1956. Tuy nhiên, vài tuần trước khi in, vào ngày 6 tháng Chín năm 1956, Michael Ventris đã bị chết trong một tai nạn giao thông. Trong khi lái xe về nhà lúc đêm khuya trên đường Great North gần Hatfield, ôtô của ông đã đâm vào một chiếc xe tải. John Chadwick đã bày tỏ lòng kính trọng đối với người bạn đồng nghiệp của mình, một bậc kỳ tài sánh ngang Champollion, và cũng là người đã chết bi thảm ở tuổi còn quá trẻ: "Công trình mà ông đã làm sẽ còn sống mãi và tên tuổi của ông sẽ còn được nhớ mãi chừng nào mà ngôn ngữ và nền văn minh Hy Lạp cổ còn được nghiên cứu".



Bảng 23. Các ký hiệu Linear B với các số tương ứng và giá trị âm của chúng

6

Alice và Bob ra công khai

Trong suốt Thế chiến Thứ hai, các nhà giải mã Anh đã có vị thế cao hơn người Đức, chủ yếu là do những người ở Bletchley Park, theo sự dẫn dắt của người Ba Lan, đã phát triển được một số công nghệ giải mã mới nhất. Ngoài các máy *bom* của Turing, được sử dụng để giải mật mã Enigma, người Anh cũng đã phát minh ra một thiết bị giải mã khác là Colossus để chống lại một dạng mã hóa thậm chí còn mạnh hơn, đó là mật mã Lorenz của Đức. Trong hai loại máy giải mã thì chính Colossus mới quyết định đến sự phát triển của khoa mật mã trong suốt nửa cuối của thế kỷ 20.

Mật mã Lorenz được sử dụng để mã hóa các thông tin liên lạc giữa Hitle và các tướng lĩnh của ông ta. Việc mã hóa được thực hiện bởi máy Lorenz SZ40, vận hành tương tự như máy Enigma song phức tạp hơn nhiều và nó đã đặt ra một thách thức lớn hơn cho các nhà giải mã ở Bletchley. Tuy nhiên, hai nhà giải mã của Bletchley là John Tiltman và Bill Tutte đã tìm ra điểm yếu trong cách sử dụng mật mã Lorenz, một sơ hở mà Bletchley có thể tận dụng và nhờ đó mà họ đọc được các thư tín của Hitle.

Hóa giải mật mã Lorenz đòi hỏi sự kết hợp của tìm kiếm, so sánh đối chiếu, phân tích thống kê và phán đoán thận trọng, tất cả đều vượt quá khả năng kỹ thuật của *bom*. *Bom* chỉ có thể thực hiện một nhiệm vụ cụ thể với tốc độ cao, song chúng không đủ linh hoạt để xử lý những tinh tế của mật mã Lorenz. Các thông tin được mã hóa bằng Lorenz phải được giải mã bằng tay, với hàng tuần nỗ lực vật vã, mà đến lúc xong thì hầu hết các thông tin đã lỗi thời. Cuối cùng, Max Newman, một nhà toán học ở Bletchley, đã nảy ra cách cơ giới hóa việc giải mã Lorenz. Chủ yếu dựa trên khái niệm của Alan Turing về máy vạn năng, Newman đã thiết kế một máy có khả năng tự thích ứng với các vấn đề khác nhau, cái mà ngày nay chúng ta gọi là máy tính lập trình.

Thực hiện thiết kế của Newman được cho là bất khả thi về mặt kỹ thuật nên các quan chức cấp cao ở Bletchley đã xếp xó dự án này. May mắn thay, Tommy Flowers, một kỹ sư đã từng tham dự các cuộc thảo luận về thiết kế của Newman, đã quyết định bất chấp thái độ hoài nghi của Bletchley, cứ tiếp tục chế tạo chiếc máy này. Tại trung tâm nghiên cứu của Bưu điện ở Dollis Hill, Bắc London, Flowers đã sử dụng bản thiết kế chi tiết của Newman và mất mười tháng để biến nó thành máy Colossus, rồi gửi nó tới Bletchley Park vào ngày 8 tháng Mười hai năm 1943. Máy sử dụng chưa tới 1.500 đèn điện tử, nhưng nhanh hơn một cách đáng kể so với những chuyển mạch dùng rơle điện cơ chậm chạp trong các máy *bom*. Song điều quan trọng hơn tốc độ của Colossus, đó là nó có thể lập trình. Chính điều này đã làm cho Colossus trở thành tiền thân của máy tính kỹ thuật số hiện đại.

Colossus, cũng như mọi thứ khác ở Bletchley Park, đều bị phá hủy sau chiến tranh, và những người làm việc với nó bị cấm

không được nói đến. Khi Tommy Flowers được yêu cầu hủy bỏ bản thiết kế Colossus, ông đã nghiêm chỉnh chấp hành mang xuống bếp và đốt chúng đi. Thế là những thiết kế máy tính đầu tiên của thế giới đã bị mất đi vĩnh viễn. Việc giữ bí mật này có nghĩa là các nhà khoa học khác được hưởng lợi từ việc phát minh ra máy tính. Năm 1945, J. Presper Eckert và John W.Mauchly ở Đại học Pennsylvania đã hoàn thành chiếc máy ENIAC *(Electronic Numerical Integrator and Calculator* - Máy tính và tích phân số điện tử), chứa tới 18.000 đèn điện tử, có thể thực hiện 5.000 phép tính trong một giây. Trong nhiều thập kỷ, ENIAC, chứ không phải là Colossus, được coi là mẹ đẻ của tất cả các máy tính.

Sau khi đóng góp cho sự ra đời của máy tính hiện đại, các nhà giải mã sau chiến tranh vẫn tiếp tục phát triển và sử dụng công nghệ máy tính để giải mã tất cả các loại mật mã. Giờ họ có thể tận dụng được tốc độ và sự linh hoạt của các máy tính lập trình để nghiên cứu tất cả các khóa mã khả dĩ cho đến khi tìm thấy khóa mã đúng. Đáp lại, các nhà tạo mã bắt đầu phản công, khai thác sức mạnh của máy tính để tạo nên những mật mã ngày càng phức tạp hơn. Tóm lại, máy tính đóng vai trò quan trọng trong cuộc chiến giữa các nhà tạo mã và giải mã sau chiến tranh.

Sử dụng máy tính để mã hóa, xét trong phạm vi lớn, cũng rất giống với các dạng mã hóa truyền thống. Thực tế thì chỉ có ba khác biệt đáng kể giữa mã hóa bằng máy tính và mã hóa cơ học vốn là cơ sở của những loại mật mã như Enigma. Sự khác biệt thứ nhất là máy mã hóa cơ học bị hạn chế bởi khả năng chế tạo trên thực tế, trong khi máy tính có thể bắt chước một máy mã trên lý thuyết với độ phức tạp cực lớn. Chẳng hạn, máy tính có thể lập trình bắt chước hoạt động của hàng trăm đĩa mã hóa,

một số đĩa quay theo chiều kim đồng hồ, một số quay ngược lại, số đĩa khác lại biến mất cứ sau mỗi 10 chữ cái, và số đĩa khác nữa lại quay ngày càng nhanh trong quá trình mã hóa. Một máy cơ học kiểu như vậy là không thể chế tạo được trong thực tế, song máy tính tương đương với nó có thể tạo được mật mã có độ an toàn cao.

Sự khác biệt thứ hai đơn giản là vấn đề tốc độ. Điện tử học có thể tạo nên những đĩa mã hóa nhanh hơn nhiều so với các đĩa mã hóa cơ học: một máy tính lập trình để bắt chước mật mã Enigma có thể mã hóa một đoạn thông tin dài trong nháy mắt. Nói cách khác, một máy tính được lập trình để thực hiện một dạng mã hóa phức tạp hơn nhiều vẫn có thể hoàn thành nhiệm vụ trong một khoảng thời gian chấp nhận được.

Thứ ba, và có lẽ là quan trọng nhất, đó là máy tính biến đổi các con số thay vì các chữ cái trong bảng chữ cái. Các máy tính chỉ xử lý các số nhị phân - là những dãy các số 1 và số 0 được gọi là các *chữ số nhị phân*, hay viết tắt là *bit* cho ngắn gọn. Trước khi mã hóa, thông tin bất kỳ phải được chuyển thành các số nhị phân. Sự chuyển đổi này có thể được thực hiện theo các quy tắc khác nhau, chẳng hạn Mã Tiêu chuẩn của Mỹ cho Trao đổi Thông tin, quen được gọi tắt là ASCII, đọc là "asskey". ASCII gán một số nhị phân gồm bảy chữ số cho mỗi chữ cái trong bảng chữ cái. Ở đây chỉ cần hiểu rằng số nhị phân đơn giản là một dãy các số 1 và số 0 xác định một cách duy nhất mỗi chữ cái (Bảng 24), cũng như mã Morse xác định mỗi chữ cái bằng một chuỗi duy nhất các dấu chấm và dấu gạch. Có 128 (2^7) cách sắp xếp bảy chữ số nhị phân, vì vậy ASCII có thể xác định tới 128 ký tự khác nhau. Điều này cho phép đủ chỗ để xác định tất cả các chữ cái viết

thường (ví dụ, **a = 1100001**), tất cả các dấu câu cần thiết (ví dụ,! **= 0100001**), cũng như các ký hiệu khác (như **& = 0100110**). Một khi thông tin đã được chuyển đổi thành các số nhị phân thì sự mã hóa bắt đầu.

Tuy chúng ta đang làm việc với các máy tính và các con số, chứ không phải các máy mã và các chữ cái, song việc mã hóa vẫn được tiến hành theo các nguyên tắc thay thế và chuyển vị như cũ, trong đó các phần tử của thông tin được thay thế bằng các phần tử khác, hoặc vị trí của chúng được hoán đổi, hoặc cả hai. Mỗi sự mã hóa, dù phức tạp đến đâu, cũng có thể phân tích thành những tổ hợp của các thao tác đơn giản này. Hai ví dụ dưới đây sẽ minh họa cho sự đơn giản rất căn bản của sự mã hóa nhờ máy tính bằng cách cho thấy máy tính có thể thực hiện một mật mã thay thế và một mật mã chuyển vị sơ cấp như thế nào.

Trước hết, hãy tưởng tượng chúng ta muốn mã hóa từ **HELLO** bằng cách dùng một phiên bản máy tính đơn giản của mã chuyển vị. Trước khi mã hóa, chúng ta phải dịch thông tin sang ASCII theo Bảng 24:

Văn bản thường = **HELLO**
= **1001000 1000101 1001100 1001100 1001111**

Một trong những dạng đơn giản nhất của mã chuyển vị đó là đổi chỗ của số thứ nhất và thứ hai, số thứ ba và thứ tư và cứ tiếp tục như vậy. Trong trường hợp này, số cuối cùng vẫn không thay đổi vì số lượng các số là lẻ. Để thấy rõ hơn quy trình này, tôi sẽ bỏ đi khoảng cách giữa các khối ASCII trong văn bản thường để tạo thành một dãy số liên tục và xếp thẳng hàng với văn bản mật mã để so sánh:

Văn bản thường = **10010001000101100110010011001001111**
Văn bản mật mã = **01100010001010011001100011000110111**

Một đặc điểm thú vị của sự chuyển vị ở cấp độ số nhị phân là việc chuyển vị này có thể xảy ra ngay trong mỗi chữ cái. Hơn nữa, các bit của một chữ cái có thể hoán đổi với các bit của chữ cái kề bên. Ví dụ, bằng cách chuyển vị số thứ 7 và thứ 8, thì số **0** cuối cùng của chữ **H** đã đổi vị trí với số 1 đầu tiên của chữ **E**. Thông tin được mã hóa là một xâu duy nhất gồm 35 bit được chuyển đến cho người nhận, người này sau đó sẽ đảo ngược lại quá trình chuyển vị để tái tạo dãy số nhị phân ban đầu. Cuối cùng, người nhận dịch các chữ số nhị phân này nhờ ASCII để có được thông tin **HELLO**.

Tiếp theo, hãy tưởng tượng chúng ta muốn mã hóa cùng một thông tin **HELLO**, nhưng lần này ta sử dụng phiên bản máy tính đơn giản của mật mã thay thế. Một lần nữa, chúng ta cũng bắt đầu bằng việc chuyển đổi thông tin thành ASCII trước khi mã hóa. Sau đó, như thường lệ, việc thay thế dựa trên một chìa khóa mã được thống nhất từ trước giữa người gửi và người nhận. Trong trường hợp này, chìa khóa mã là **DAVID** được dịch ra ASCII, và được sử dụng như sau. Mỗi yếu tố trong văn bản thường được "cộng" với yếu tố tương ứng của chìa khóa mã. Việc cộng các số nhị phân cần được tuân theo hai quy tắc đơn giản. Nếu các yếu tố trong văn bản thường và chìa khóa mã giống nhau thì yếu tố trong văn bản thường sẽ được thay thế bằng số **0** trong văn bản mật mã. Song nếu các yếu tố trong văn bản thường và chìa khóa mã khác nhau thì yếu tố trong văn bản thường được thay thế bằng số **1** trong văn bản mật mã:

Thông tin	HELLO
Thông tin trong ASCII	10010001000101100110010011001001111
Chìa khóa mã = DAVID	10001001000001101011010010011000100
Văn bản mật mã	00011000000100001101000001010001011

Thông tin được mã hóa là một dãy duy nhất gồm 35 chữ số nhị phân được chuyển đến cho người nhận, người này sẽ sử dụng cùng một chìa khóa mã để đảo ngược sự thay thế, tái tạo lại dãy các chữ số nhị phân ban đầu. Cuối cùng, người nhận dịch lại các chữ số nhị phân này qua ASCII để có được thông tin **HELLO.**

Việc mã hóa bằng máy tính bị giới hạn trong số những người có máy tính thôi, mà trong thời kỳ đầu tiên thì có nghĩa là chỉ chính phủ và quân đội mới có. Tuy nhiên, một loạt các đột phá về khoa học, công nghệ và kỹ thuật đã khiến máy tính, và cả việc mã hóa bằng máy tính nữa đã trở nên khả dụng một cách rộng rãi hơn. Năm 1947, Phòng thí nghiệm AT&T Bell đã phát minh ra tranzito (đèn bán dẫn), một linh kiện rẻ hơn thay thế cho đèn điện tử. Máy tính thương mại đã trở thành hiện thực vào năm 1951 khi các công ty như Ferranti bắt đầu sản xuất máy tính theo đơn đặt hàng. Năm 1953, IBM chào bán máy tính đầu tiên của hãng và bốn năm sau, hãng giới thiệu Fortran, một ngôn ngữ lập trình cho phép người "bình thường" cũng viết được chương trình máy tính. Sau đó, vào năm 1959, việc phát minh ra mạch tích hợp đã mở ra một kỷ nguyên mới của máy tính.

Trong suốt những năm 1960, máy tính trở nên mạnh hơn và đồng thời cũng rẻ hơn. Các hãng kinh doanh ngày càng có khả năng chi phí cho máy tính và sử dụng chúng để mã hóa các thông

tin quan trọng của mình như chuyển tiền hay những cuộc thương thảo bí mật. Tuy nhiên, khi ngày càng nhiều hãng mua máy tính và khi việc mã hóa trong giới kinh doanh lan rộng thì các nhà tạo mã lại phải đối mặt với những vấn đề mới, những khó khăn không tồn tại khi khoa học mật mã chỉ dành riêng cho chính phủ và quân đội. Một trong những lo ngại cơ bản đó là vấn đề về tiêu chuẩn hóa. Một công ty có thể sử dụng hệ thống mã hóa riêng để bảo đảm an toàn cho thông tin nội bộ của mình song không thể gửi một thông tin bí mật đến cho một tổ chức bên ngoài trừ phi người nhận cũng sử dụng cùng hệ thống mã hóa đó. Cuối cùng, vào ngày 15 tháng Năm năm 1973, Cục Tiêu chuẩn Quốc gia Hoa Kỳ đã lên kế hoạch giải quyết vấn đề này, và chính thức yêu cầu đề xuất một hệ thống mã hóa chuẩn cho phép giới kinh doanh có thể trao đổi bí mật với nhau.

Bảng 24. Các số nhị phân biểu diễn chữ cái in hoa của ASCII

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Một trong các thuật toán mật mã uy tín hơn cả và là một ứng viên cho tiêu chuẩn, đó là sản phẩm của IBM có tên là Lucifer. Nó được phát minh bởi Horst Feistel, một người Đức di cư đến Mỹ năm 1934. Ông đã sắp trở thành công dân Hoa Kỳ thì đúng lúc Mỹ tham gia cuộc chiến, mà điều này có nghĩa là ông bị quản thúc tại gia cho đến năm 1944. Trong vài năm sau đó, ông đã phải từ bỏ sở thích về mật mã của mình để tránh gây sự nghi ngờ của các nhà chức trách Mỹ. Khi cuối cùng ông bắt đầu nghiên cứu trở lại về mật mã, tại Trung tâm Nghiên cứu Không lực ở Cambridge, ông nhanh chóng nhận ra rằng mình đã gặp rắc rối với Cơ quan An ninh Quốc gia (NSA), một tổ chức chịu trách nhiệm chung về việc duy trì an ninh thông tin liên lạc của chính phủ và quân đội, và cũng là tổ chức tìm mọi cách để chặn bắt và giải mã các thông tin liên lạc của nước ngoài. NSA tuyển dụng nhiều nhà toán học, mua nhiều phần cứng máy tính và chặn được nhiều thông tin hơn bất kỳ tổ chức nào khác trên thế giới. Nó là tổ chức hàng đầu thế giới trong việc rình mò.

NSA không chú ý đến quá khứ của Feistel mà chỉ muốn độc quyền nghiên cứu về mật mã và dường như là họ đã can thiệp để các dự án nghiên cứu của Feistel bị hủy bỏ. Trong những năm 1960, Feistel đã chuyển đến Tập đoàn Mitre, song NSA vẫn tiếp tục gây áp lực và buộc ông phải từ bỏ công việc của mình một lần nữa. Và cuối cùng, Feistel đã trụ lại tại Phòng Thí nghiệm Thomas J.Watson của IBM ở gần New York, nơi mà trong vài năm, ông đã có thể tiến hành những nghiên cứu của mình mà không bị quấy rầy. Cũng chính ở đó, vào đầu những năm 1970, ông đã phát minh ra hệ thống Lucifer.

Lucifer mã hóa các thông tin theo quy trình như sau. Trước tiên, thông tin được dịch thành một xâu dài các chữ số nhị phân. Thứ hai, dãy này được tách thành các khối gồm 64 chữ số và việc mã hóa được thực hiện riêng biệt ở từng khối một. Thứ ba, ở mỗi khối, 64 chữ số được xáo trộn và sau đó lại được chia thành hai nửa khối gồm 32 chữ số được ký hiệu là $Trái^0$ và $Phải^0$. Các chữ số trong $Phải^0$ sau đó được cho qua "hàm xáo trộn", hàm này biến đổi các chữ số theo một cơ chế thay thế phức tạp. Phần $Phải^0$ sau khi được xáo trộn lại được ghép vào $Trái^0$ để tạo nên một nửa khối mới gồm 32 chữ số được gọi là $Phải^1$. $Trái^0$ ban đầu giờ lại được đặt lại là $Trái^1$. Toàn bộ quá trình này được gọi là một "vòng". Nó được lặp lại ở vòng 2, song bắt đầu với các khối mới là $Phải^1$ và $Trái^1$ và kết thúc với $Trái^2$ và $Phải^2$ và cứ được lặp lại như thế cho đến khi đạt tổng số 16 vòng. Quá trình mã hóa cũng gần giống như nhào một tảng bột. Hãy tưởng tượng một tảng bột dài với thông tin được viết trên nó. Đầu tiên, tảng bột được chia thành các đoạn dài 64 cm. Sau đó, một nửa của một đoạn được lấy ra, nhào, cuộn lại rồi nhập vào với nửa kia và kéo dài ra thành một đoạn mới. Quá trình này tiếp tục cho đến khi thông tin đã hoàn toàn bị xáo trộn. Sau 16 lần nhào trộn, mật mã được gửi đi và giải mã bằng cách đảo ngược lại quá trình.

Chi tiết chính xác của hàm xáo trộn có thể thay đổi và được quyết định bởi một chìa khóa mã đã được thống nhất giữa người gửi và người nhận. Nói cách khác, cùng một thông tin có thể được mã hóa theo vô số cách khác nhau phụ thuộc vào chìa khóa mã nào được lựa chọn. Các chìa khóa mã được sử dụng trong mật mã máy tính chỉ đơn giản là các con số. Vì vậy, người gửi và người nhận chỉ cần thống nhất con số nào được quyết định

làm chìa khóa mã. Sau đó, việc mã hóa đòi hỏi người gửi phải nạp số chìa khóa mã và thông tin vào Lucifer, và nó sẽ cho ra văn bản mật mã. Việc giải mã đòi hỏi người nhận phải nạp vào Lucifer cùng số chìa khóa mã và văn bản mật mã để có được thông tin ban đầu.

Lucifer nói chung được xem là một trong những sản phẩm mã hóa thương mại khả dụng mạnh nhất, và kết quả là nó được rất nhiều tổ chức sử dụng. Ai cũng tưởng rằng tất yếu hệ thống mã hóa này sẽ được chấp nhận là tiêu chuẩn của Mỹ song một lần nữa NSA lại can thiệp vào công việc của Feistel. Lucifer mạnh đến nỗi nó có thể làm cho tiêu chuẩn mã hóa nằm ngoài khả năng giải mã của NSA; vì vậy không có gì đáng ngạc nhiên khi NSA không muốn thấy một tiêu chuẩn mã hóa mà họ không thể phá vỡ được. Vì vậy, có tin đồn là NSA đã vận động hành lang để làm yếu đi một khía cạnh của Lucifer, đó là số chìa khóa mã khả dĩ, trước khi cho phép nó được công nhận là tiêu chuẩn.

Số chìa khóa mã khả dĩ là một trong những nhân tố quan trọng quyết định đến sức mạnh của một mật mã. Một nhà giải mã định phá một thông tin được mã hóa phải kiểm tra tất cả các chìa khóa mã khả dĩ, và số lượng chìa khóa mã tiềm năng càng lớn thì thời gian tìm ra chìa khóa đúng càng dài. Nếu chỉ có 1.000.000 chìa khóa mã tiềm năng thì một nhà giải mã có thể sử dụng một máy tính mạnh để tìm thấy chìa khóa đúng chỉ trong vài phút, và nhờ đó giải được thông tin mã hóa. Tuy nhiên, nếu số chìa khóa mã khả dĩ đủ lớn, thì việc tìm được chìa khóa mã đúng là chuyện phi thực tế. Nếu Lucifer trở thành tiêu chuẩn mã hóa thì NSA muốn bảo đảm rằng nó vận hành chỉ với một số lượng chìa khóa mã hạn chế.

NSA ủng hộ việc giới hạn số chìa khóa mã vào khoảng 100.000.000.000.000.000 (về kỹ thuật tương đương với 56 bit, vì nó bao gồm 56 chữ số khi được viết ở dạng nhị phân). Dường như NSA tin rằng một chìa khóa mã như vậy sẽ mang lại an toàn cho cộng đồng, vì không tổ chức dân sự nào có máy tính đủ mạnh để kiểm tra mỗi chìa khóa mã tiềm năng trong một khoảng thời gian hợp lý. Tuy nhiên, bản thân NSA, nhờ tiếp cận được với nguồn máy tính mạnh nhất thế giới, sẽ có thể giải mã được chúng. Hệ mật mã 56 bit Lucifer của Feistel đã chính thức được thông qua vào ngày 23 tháng Mười một năm 1976, và được gọi là Tiêu chuẩn Mã hóa Dữ liệu (DES). Một phần tư thế kỷ sau, DES vẫn còn là tiêu chuẩn mã hóa chính thức của Hoa Kỳ.

Việc thông qua DES đã giải quyết được vấn đề chuẩn hóa, khuyến khích các hãng kinh doanh sử dụng mật mã để đảm bảo an toàn. Hơn nữa, DES lại đủ mạnh để chống lại sự tấn công của các đối thủ kinh doanh. Một công ty với máy tính bình thường không thể đột nhập được vào các thông tin mã hóa bằng DES vì số chìa khóa khả dĩ là đủ lớn. Tiếc thay, mặc dù được tiêu chuẩn hóa và mặc dù DES có mạnh đi nữa thì các hãng vẫn phải đối mặt với một vấn đề quan trọng hơn, đó là vấn đề *phân phối chìa khóa mã*.

Bạn hãy hình dung một ngân hàng muốn gửi một số dữ liệu mật cho một khách hàng qua đường dây điện thoại song lại lo ngại rằng có thể có ai đó đặt máy ghi âm trộm. Ngân hàng lựa chọn một chìa khóa mã và sử dụng DES để mã hóa thông tin dữ liệu. Để giải mã thông tin, khách hàng không chỉ cần một phần mềm DES trong máy tính của mình mà còn phải biết chìa khóa mã nào đã được sử dụng để mã hóa thông tin. Ngân hàng làm

thế nào để thông báo chìa khóa mã cho khách hàng? Nó không thể gửi chìa khóa mã qua đường dây điện thoại vì nghi ngờ có máy nghe trộm. Chỉ có một cách thực sự an toàn đó là đưa tận tay khách hàng, một nhiệm vụ rõ ràng là tốn nhiều thời gian. Một giải pháp ít an toàn hơn nhưng thực tế hơn là gửi chìa khóa mã qua người đưa thư. Trong những năm 1970, các ngân hàng đã thử phân phối chìa khóa mã bằng cách tuyển dụng những người đưa thư đặc biệt, được lựa chọn chặt chẽ trong số những nhân viên đáng tin cậy nhất của công ty. Họ rong ruổi khắp thế giới với những chiếc vali có khóa móc, đưa chìa khóa mã tận tay từng khách hàng, những người sẽ nhận được thông tin từ ngân hàng vào tuần sau đó. Khi quy mô hệ thống kinh doanh lớn mạnh lên, ngày càng nhiều thông tin được gửi đi và ngày càng nhiều chìa khóa mã phải phân phối, các ngân hàng nhận thấy quá trình phân phối này trở thành một cơn ác mộng khủng khiếp và tổng chi phí quá cao khó có thể trang trải được.

Vấn đề phân phối chìa khóa mã cũng đã từng gây khó khăn cho các nhà mật mã trong lịch sử. Chẳng hạn, trong suốt Thế chiến Thứ hai, Tổng hành dinh cấp cao của Đức đã phải phân phối sổ khóa mã ngày hàng tháng cho tất cả những người điều khiển Enigma, một vấn đề cực lớn về mặt hậu cần. Tương tự như vậy, các tàu ngầm Đức, thường xuyên xa bờ trong một khoảng thời gian dài, cũng cần được cung cấp chìa khóa mã định kỳ bằng một cách nào đó. Trước kia, những người sử dụng mật mã Vigenère cũng phải tìm cách chuyển từ chìa khóa từ người gửi đến người nhận. Bất kể mật mã có độ an toàn như thế nào đi nữa về mặt lý thuyết nhưng trong thực tế vấn đề phân phối chìa khóa mã có thể lại là một điểm yếu của nó.

Trong phạm vi nào đó, chính phủ và quân đội có thể giải quyết được vấn đề này nhờ đổ tiền của và nguồn lực vào đó. Thông tin của họ quan trọng đến mức họ sẽ làm bất cứ điều gì có thể để bảo đảm cho việc phân phối chìa khóa mã được an toàn. Chìa khóa mã của Chính phủ Hoa Kỳ được quản lý và phân phối bởi COMSEC, viết tắt của Cơ quan An ninh Thông tin liên lạc. Trong những năm 1970, COMSEC chịu trách nhiệm chuyển hàng tấn chìa khóa mã mỗi ngày. Khi các con tàu mang tài liệu của COMSEC đến bến cảng, những người coi giữ mật mã sẽ lên tàu, thu nhận các chồng thẻ, các băng giấy, các đĩa mềm, hay bất kỳ chìa khóa mã trung gian nào khác có thể dự trữ và sau đó chuyển chúng đến những người nhận đã được định trước.

Phân phối chìa khóa mã có vẻ như là một công việc tầm thường song nó đã trở thành một vấn đề nan giải đối với các nhà mật mã sau chiến tranh. Nếu hai tổ chức muốn liên lạc một cách bí mật, họ phải dựa vào một tổ chức thứ ba để chuyển chìa khóa mã và điều này có thể trở thành một mắt xích yếu nhất trong chuỗi an toàn. Tình trạng tiến thoái lưỡng nan này của các hãng kinh doanh là rất dễ hiểu - nếu chính phủ với tất cả tiền bạc của họ mà còn phải vật lộn để bảo đảm an toàn cho việc phân phối chìa khóa mã, thì làm thế nào các công ty của thường dân lại có thể hy vọng đạt được một sự phân phối chìa khóa mã đáng tin cậy mà chính họ không bị phá sản?

Mặc dù có những tuyên bố rằng vấn đề phân phối chìa khóa mã là không thể giải quyết được, song một nhóm những người không chịu khuất phục đã chiến thắng mọi nghịch cảnh và đã tìm ra một giải pháp tuyệt vời vào giữa những năm 1970. Họ đã phát minh ra một hệ thống dường như phá vỡ mọi quy tắc

logic. Mặc dù máy tính đã làm biến đổi việc thực hiện các mật mã, song cuộc cách mạng vĩ đại nhất của khoa mật mã thế kỷ 20 lại chính là việc phát triển các kỹ thuật để giải quyết vấn đề phân phối chìa khóa mã. Thực tế, phát minh này được coi như là một thành tựu về mật mã vĩ đại nhất kể từ phát minh ra mật mã dùng một bảng chữ cái từ hơn 2000 năm trước.

Thánh nhân đãi kẻ khù khờ

Whitfield Diffie là một trong những nhà tạo mã hăm hở nhất ở thế hệ ông. Nhìn bề ngoài ông tạo ra một hình ảnh thật ấn tượng và phần nào hơi mâu thuẫn. Trang phục không chê vào đâu được của ông cho thấy hầu như suốt những năm 1990, ông làm việc cho một trong những công ty lớn nhất nước Mỹ - công việc chính thức hiện thời của ông là kỹ sư cao cấp của hãng Sun Microsystems. Tuy nhiên, mái tóc dài ngang vai và bộ râu trắng dài lại cho thấy trái tim ông vẫn thuộc về những năm 1960. Ông dành nhiều thời gian cho phòng máy tính song trông ông rất thư thái như thể ở trong một *ashram* ở Bombay (*ashram* là nơi các thầy tu ở và truyền đạo ở Ấn Độ, có thể là một hang nhỏ trong núi hoặc lều tre). Diffie ý thức rõ rằng trang phục và cá tính của ông thực sự rất ấn tượng đối với người khác và nhận xét rằng, "Người ta luôn nghĩ tôi cao hơn chiều cao thực của tôi, và họ nói đấy là hiệu ứng con Hổ - "Bất kể cân nặng của nó là bao nhiêu, trông nó vẫn luôn to lớn hơn bởi bước đi nhún nhảy của nó".

Diffie sinh năm 1944, và dành hầu hết những năm đầu của mình ở Queens, New York. Khi còn là một đứa trẻ, ông đã rất say mê toán học, đọc từ cuốn *Sách tra cứu các bảng Toán học của Công*

Whitfield Diffie

ty Hóa chất Cao su đến cuốn *Con đường của Toán học thuần túy* của G. H. Hardy. Rồi ông tiếp tục học toán ở Viện Công nghệ Massachusetts (MIT), và tốt nghiệp năm 1965. Sau đó ông đã làm nhiều công việc có liên quan đến an ninh máy tính và đến đầu những năm 1970, ông đã trưởng thành và trở thành một trong số ít những chuyên gia an ninh độc lập thực sự, một nhà tạo mã mang tư tưởng tự do, không làm việc cho chính phủ cũng như bất kỳ một tập đoàn lớn nào. Theo cách gọi sau này, ông là một *cypherpunk* đầu tiên (thuật ngữ này do Jude Milhon đưa ra từ trò chơi chữ của từ *cyberpunk*, có nghĩa là những người sử dụng mật mã, họ tạo thành nhóm và các cá nhân trao đổi với nhau bằng mật mã - ND).

Diffie đặc biệt quan tâm đến vấn đề phân phối chìa khóa mã, và ông biết rằng ai tìm ra được một giải pháp sẽ đi vào lịch sử như một trong những nhà tạo mã vĩ đại của mọi thời đại. Diffie bị vấn đề này lôi cuốn đến mức nó là một trong những mục quan trọng nhất trong cuốn sổ tay đặc biệt của ông có tựa đề *Những Bài toán của một Lý thuyết đầy Tham vọng của Khoa học mật mã*. Một phần động cơ của Diffie đến từ sự quan sát của ông về một thế giới được kết nối với nhau. Trở lại những năm 1960, Bộ Quốc phòng Mỹ bắt đầu tài trợ cho một tổ chức nghiên cứu được gọi

là Cơ quan Dự án Nghiên cứu Tiên tiến (ARPA), và một trong các dự án hàng đầu của ARPA là tìm ra cách nối mạng các máy tính quân sự trên những khoảng cách lớn. Nó cho phép một máy tính khi bị hỏng có thể chuyển nhiệm vụ của nó sang một máy tính khác trong hệ thống. Mục đích chính là làm cho cơ sở hạ tầng máy tính của Lầu Năm Góc mạnh hơn trước sự tấn công hạt nhân, song hệ thống cũng cho phép các nhà khoa học gửi thông tin cho nhau, và thực hiện các tính toán nhờ khai thác công suất còn dư thừa của các máy tính ở xa. ARPANet được lập ra vào năm 1969 và đến cuối năm đó, đã có bốn vị trí được nối mạng. ARPANet lớn mạnh đều đặn về quy mô và tới năm 1982, nó đã sinh ra Internet. Vào cuối những năm 1980, không chỉ ở trong các cơ quan chính phủ và khoa học, mà ai cũng có thể truy cập Internet, và vì vậy số lượng người sử dụng bùng nổ. Ngày nay, hơn một trăm triệu người sử dụng Internet để trao đổi thông tin và gửi thư điện tử.

Trong khi ARPANet vẫn còn trong trứng nước, Diffie đã nhìn xa khi tiên đoán rằng xa lộ thông tin và cuộc cách mạng kỹ thuật số sớm muộn gì rồi cũng sẽ tới. Một ngày nào đó, người bình thường cũng sẽ có máy tính riêng và các máy tính này sẽ được nối với nhau qua đường dây điện thoại. Diffie tin rằng nếu con người sau này được sử dụng máy tính để trao đổi thư điện tử thì họ sẽ có quyền được mã hóa các thông tin để bảo vệ bí mật của mình. Tuy nhiên, việc mã hóa đòi hỏi phải có sự trao đổi chìa khóa mã thật an toàn. Nếu chính phủ và các tập đoàn lớn còn gặp rắc rối trong việc phân phối chìa khóa mã thì công chúng lại càng không thể làm được và sẽ thực sự bị tước đi cái quyền được riêng tư của mình.

Diffie đã hình dung ra hai người xa lạ gặp nhau trên Internet và tự hỏi làm thế nào để họ có thể gửi cho nhau một thông tin được mã hóa. Ông cũng nghĩ đến chuyện một người muốn mua hàng trên Internet. Làm thế nào để người đó gửi một thư điện tử có các thông tin chi tiết về thẻ tín dụng mà chỉ người bán hàng trên Internet mới có thể giải mã được chúng? Trong cả hai trường hợp, hai bên đều cần phải chia sẻ một chìa khóa mã, song làm thế nào họ có thể trao đổi chìa khóa mã một cách bí mật? Số các hợp đồng bình thường và lượng thư điện tử tự phát sẽ là rất lớn và điều đó có nghĩa là việc phân phối chìa khóa mã sẽ là phi thực tế. Diffie lo sợ rằng khó khăn trong phân phối chìa khóa mã sẽ hạn chế việc sử dụng bí mật riêng tư kỹ thuật số của công chúng, và ông trở nên bị ám ảnh với ý nghĩ phải tìm ra một cách giải quyết vấn đề đó.

Năm 1974, Diffie, khi đó vẫn còn là một nhà tạo mã lưu động, đã đến thăm Phòng thí nghiệm Thomas J. Watson của IBM, nơi ông được mời đến để nói chuyện. Ông đã nói về rất nhiều chiến lược tấn công khác nhau vào vấn đề phân phối chìa khóa mã, song tất cả các ý tưởng đó của ông mới chỉ là dự định, và các thính giả vẫn hoài nghi về viễn cảnh có được một giải pháp. Chỉ có một phản ứng tích cực duy nhất đối với bài trình bày của Diffie là của Alan Konheim, một trong các chuyên gia cao cấp về khoa học mật mã của IBM, người đã nhắc đến một người khác cũng vừa đến thăm phòng thí nghiệm và trong bài nói chuyện cũng đã đề cập đến vấn đề phân phối chìa khóa mã. Người đó là Martin Hellman, một giáo sư đến từ trường Đại học Stanford ở California. Tối hôm đó, Diffie đã lái xe đi một chặng đường 5.000km đến Bờ Tây để gặp người duy nhất dường như có cùng

nỗi ám ảnh với ông. Sự liên minh giữa Diffie và Hellman đã trở thành một trong những mối quan hệ hợp tác năng động nhất trong khoa học mật mã.

Martin Hellman sinh năm 1945 tại khu phố người Do Thái, ở Bronx, song khi lên bốn, gia đình ông lại chuyển đến khu phố chủ yếu gồm những người dân gốc Ireland theo đạo Thiên chúa. Theo Hellman, sự kiện này đã làm thay đổi một cách căn bản thái độ của ông đối với cuộc đời: "Những đứa trẻ khác đi đến nhà thờ và chúng được dạy rằng người Do Thái đã giết chết Chúa, vì vậy tôi bị gọi là 'kẻ giết Chúa'. Tôi cố sức chống lại. Để bắt đầu, tôi muốn giống như mọi đứa trẻ khác, tôi muốn có một cây thông Giáng sinh và quà Giáng sinh. Nhưng sau đó tôi nhận ra rằng mình không thể giống với tất cả những đứa trẻ khác, và để tự vệ tôi giữ thái độ "Ai thèm giống như tất cả các người chứ?". Hellman theo đuổi niềm say mê của mình đối với mật mã cũng là với mong ước giữ được sự khác biệt này. Đồng nghiệp của ông đã bảo ông là điên khi nghiên cứu về khoa học mật mã vì ông sẽ phải cạnh tranh với NSA và ngân sách hàng tỉ đôla của họ. Làm sao ông có thể hy vọng khám phá ra điều gì đó mà họ chưa biết? Và nếu ông có thực sự khám phá ra điều gì đó, thì NSA cũng sẽ tuyên bố là tài liệu mật và xếp vào két sắt.

Ngay khi Hellman mới bắt đầu nghiên cứu, ông tình cờ đọc được cuốn *Các nhà giải mã* của nhà sử học David Kahn. Đây là cuốn phân tích chi tiết đầu tiên về sự phát triển của mật mã và nó như là một cuốn sách vỡ lòng tuyệt vời cho những nhà tạo mã tài năng bắt đầu nảy nở. *Các nhà giải mã* là người bạn đồng hành nghiên cứu duy nhất của Hellman cho mãi đến tháng Chín năm 1974, khi ông nhận được cú điện thoại bất ngờ của Whitfield

Diffie, người vừa mới lái xe xuyên lục địa để đến gặp ông. Hellman chưa bao giờ nghe nói đến Diffie song cũng miễn cưỡng đồng ý sắp xếp một cuộc hẹn trong nửa giờ vào chiều muộn ngày hôm đó. Cuối cuộc gặp, Hellman nhận ra rằng Diffie là người hiểu biết nhất mà ông từng gặp. Hai bên lập tức có cảm tình với nhau. Hellman nhớ lại: "Tôi đã hứa với vợ là sẽ về nhà trông bọn trẻ, vì vậy ông ấy đã về nhà cùng với tôi và chúng tôi ăn tối cùng nhau. Ông ấy ra đi vào lúc nửa đêm. Cá tính của tôi và ông ấy rất khác nhau - ông ấy phản văn hóa hơn tôi nhiều - song cuối cùng thì sự va chạm về cá tính lại có tính cộng sinh. Đối với tôi điều đó giống như hít một luồng không khí trong lành. Làm việc trong môi trường chân không quả là hết sức khó khăn."

Vì Hellman không có nhiều kinh phí nên ông không thể chi trả cho việc thuê người bạn cùng chí hướng mới như một nghiên cứu viên. Thay vì thế, Diffie đăng ký như một nghiên cứu sinh. Cùng với nhau, Hellman và Diffie bắt đầu nghiên cứu vấn đề phân phối chìa khóa mã, họ cố gắng không mệt mỏi để tìm ra một cách thức có thể thay thế cho việc chuyên chở chìa khóa mã bằng con người một cách mệt nhọc qua những khoảng cách lớn. Trong quá trình đó, họ đã cộng tác với Ralph Merkle. Merkle là một người tị nạn về trí tuệ, ông di cư đến từ một nhóm nghiên cứu khác mà giáo sư ở đó không đồng cảm với giấc mơ giải quyết vấn đề phân phối chìa khóa mã, một vấn đề được coi là bất khả. Hellman kể:

> Cũng giống như chúng tôi, Ralph sẵn lòng làm một thằng ngốc. Và con đường đạt tới đỉnh cao thông qua sự triển khai nghiên cứu lại từ đầu phải là của kẻ ngốc vì chỉ có ngốc mới kiên trì thử mãi như vậy. Anh có ý tưởng số 1, anh rất phấn khích,

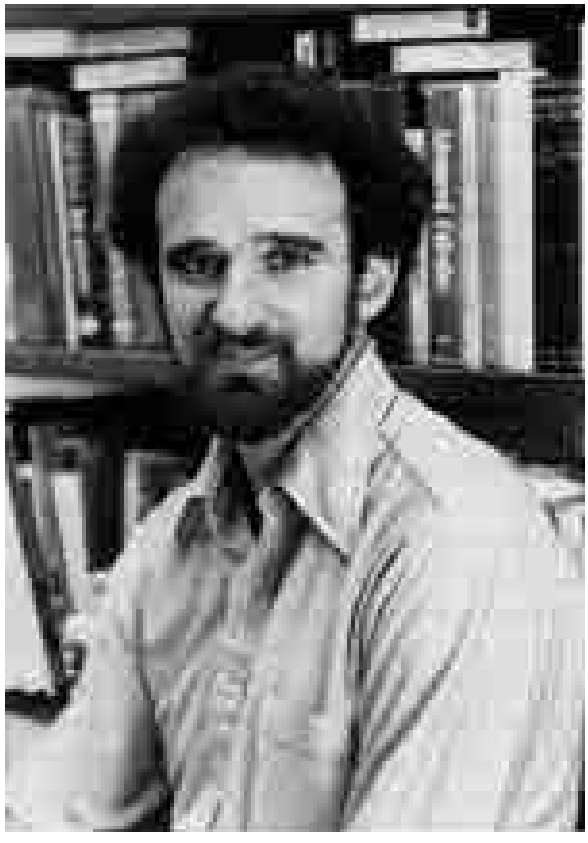
và rồi nó thất bại. Sau đó anh lại nảy ra ý tưởng số 2, anh rất hứng khởi, nhưng rồi nó lại thất bại. Rồi anh có ý tưởng số 99, anh lại rất hứng khởi, nhưng nó cũng lại thất bại nốt. Chỉ có kẻ ngốc mới hứng khởi đến ý tưởng thứ 100, nhưng rất có thể phải mất đến 100 ý tưởng thì người ta mới được đền đáp. Trừ phi anh đủ ngốc để tiếp tục hứng khởi, nếu không thì anh làm gì có động cơ, làm gì có năng lượng để đi tiếp. Quả là Chúa ban thưởng cho những thằng ngốc.

Toàn bộ vấn đề phân phối chìa khóa mã là một tình huống kiểu *catch-22* cổ điển*. Nếu hai người muốn trao đổi thông tin bí mật qua điện thoại, người gửi phải mã hóa nó. Để mã hóa thông tin, người gửi phải sử dụng chìa khóa mã mà bản thân nó cũng lại là bí mật, vì vậy mới nảy sinh vấn đề là làm sao chuyển chìa khóa mã bí mật cho người nhận để truyền đi thông tin bí mật. Tóm lại, trước khi hai người có thể trao đổi một bí mật (một bức thư mã hóa), họ đã phải chia sẻ một bí mật khác (chìa khóa mã).

Khi xét đến vấn đề phân phối chìa khóa mã, để cho dễ hình dung, ta coi Alice, Bob và Eve, ba nhân vật hư cấu, những người đã trở thành tiêu chuẩn công nghiệp để thảo luận về khoa học mật mã. Trong một tình huống điển hình, Alice muốn gửi một bức thư cho Bob hay ngược lại, còn Eve thì đang cố nghe lén. Nếu Alice muốn gửi các bức thư riêng cho Bob, cô ta sẽ mã hóa từng cái trước khi gửi, mỗi lần sử dụng một chìa khóa mã khác nhau. Alice phải đối mặt với vấn đề phân phối chìa khóa mã

---

* *Catch-22*, tiểu thuyết của Joseph Heller (1961) và từ này hiện được sử dụng rộng rãi với hàm ý một chuỗi những sự kiện mà trong đó sự kiện này phụ thuộc vào sự kiện khác và đến lượt nó lại phụ thuộc vào sự kiện ban đầu. (ND)



Martin Hellman

vì cô phải chuyển chìa khóa mã cho Bob một cách bí mật, nếu không anh ta sẽ không thể giải mã được bức thư. Một cách để giải quyết vấn đề này là Alice và Bob gặp nhau trực tiếp một tuần một lần và trao đổi đủ số chìa khóa mã cho các bức thư sẽ gửi trong vòng bảy ngày sau đó. Trao đổi chìa khóa mã trực tiếp chắc chắn là an toàn, song lại không thuận tiện, nếu như Alice hoặc Bob bị ốm chẳng hạn, thì hệ thống sẽ bị đổ vỡ. Một cách khác là Alice và Bob thuê người chuyển hộ, như thế sẽ ít an toàn hơn và lại đắt hơn, song ít nhất thì họ cũng ủy thác được phần nào công việc. Dù theo cách nào thì việc phân phối chìa khóa mã là điều không thể tránh khỏi. Trong suốt hai ngàn năm, điều này được xem như là một tiên đề của khoa mật mã - tức là một sự thật không phải bàn cãi. Tuy nhiên, có một thí nghiệm tưởng tượng dường như như thách thức tiên đề này.

Hãy tưởng tượng rằng Alice và Bob sống trong cùng một đất nước nơi mà hệ thống bưu điện là hoàn toàn phi đạo đức, những nhân viên bưu điện có thể đọc bất cứ thông tin nào không được bảo đảm. Một hôm, Alice muốn gửi một bức thư rất riêng tư cho Bob. Cô bỏ thư vào một hộp sắt, đóng lại và bảo vệ nó bằng khóa móc và chìa khóa. Cô gửi hộp có khóa móc ở bưu điện và giữ lại

chìa khóa. Tuy nhiên, khi cái hộp đến chỗ Bob, anh không thể mở được nó ra vì không có chìa khóa. Alice có tính đến chuyện bỏ chìa khóa vào một cái hộp khác, khóa lại và gửi đến cho Bob, song không có chìa khóa thì Bob cũng không thể mở được chiếc hộp thứ hai và vì vậy không thể lấy được chìa khóa để mở hộp thứ nhất. Chỉ có một cách là Alice đánh một chiếc chìa khóa nữa và đưa trước cho Bob khi họ gặp nhau lúc uống cà phê. Cho đến đây, tôi đã kể lại một câu chuyện cũ chỉ có điều là theo một kịch bản mới. Tránh việc phân phối chìa khóa mã dường như là một điều không thể về mặt logic - chắc chắn rồi, vì nếu Alice muốn khóa thứ gì đó trong hộp mà chỉ có Bob mới mở được thì cô ấy phải đưa cho anh ta một chìa khóa khác. Trao đổi chìa khóa là một phần không thể thiếu trong việc mã hóa - hay là không phải như vậy?

Bây giờ hãy hình dung một kịch bản sau. Cũng như trước, Alice muốn gửi một bức thư rất riêng tư cho Bob. Một lần nữa, cô lại bỏ thư vào một hộp sắt, khóa nó lại và gửi đến cho Bob. Khi hộp đến nơi, Bob sẽ thêm vào đó một khóa móc của mình và gửi lại cho Alice. Khi Alice nhận được chiếc hộp thì nó rất an toàn vì có cả hai khóa trên đó. Cô mở khóa của mình ra, nhưng giữ nguyên chiếc khóa của Bob để đảm bảo an toàn cho chiếc hộp. Cuối cùng cô gửi chiếc hộp lại cho Bob. Và lúc này có sự khác biệt rất quan trọng: Bob có thể mở được hộp vì nó được bảo đảm an toàn bằng khóa của chính anh, cái khóa mà chỉ mình anh có chìa.

Hàm ý của câu chuyện nhỏ này là rất lớn. Nó chứng minh rằng một thông tin bí mật có thể trao đổi một cách an toàn giữa hai người mà không cần thiết phải trao đổi chìa khóa mã. Lần

đầu tiên chúng ta có được một gợi ý rằng trao đổi chìa khóa mã không phải là một phần tất yếu của khoa mật mã. Chúng ta có thể diễn giải lại câu chuyện này thông qua việc mã hóa. Alice sử dụng chính chìa khóa mã của mình để mã hóa một bức thư gửi cho Bob, đến lượt mình, Bob lại mã hóa nó bằng chìa khóa của mình rồi gửi trả lại. Khi Alice nhận được bức thư được mã hóa hai lần, cô bỏ đi mã hóa của mình và gửi lại cho Bob, và anh này sau đó sẽ giải mã của chính mình và có thể đọc được bức thư.

Dường như vấn đề phân phối chìa khóa mã đã có thể được giải quyết vì cơ chế mã hóa kép không đòi hỏi phải trao đổi chìa khóa mã. Tuy nhiên, có một trở ngại cơ bản đối với việc thực hiện một hệ thống mà trong đó Alice mã hóa, Bob mã hóa, Alice giải mã, Bob giải mã. Vấn đề là ở trình tự tiến hành mã hóa và giải mã. Nói chung, trình tự mã hóa và giải mã là rất quan trọng, và phải tuân thủ quy tắc "vào sau ra trước". Nói cách khác, bước mã hóa cuối cùng sẽ phải giải mã đầu tiên. Trong kịch bản trên, Bob thực hiện bước mã hóa cuối cùng, vì vậy lẽ ra nó sẽ phải được giải mã trước, song ở đây chính Alice lại là người giải mã trước rồi mới đến Bob. Sự quan trọng của trình tự dễ hình dung nhất khi quan sát những việc chúng ta làm hằng ngày. Buổi sáng chúng ta đi tất vào trước rồi sau đó mới đi giày, và buổi tối, chúng ta cởi giày ra trước rồi mới cởi tất - không thể cởi tất trước khi cởi giày. Chúng ta phải tuân thủ châm ngôn "vào sau ra trước".

Đối với một số mật mã rất sơ cấp, như mật mã Ceasar, chúng đơn giản đến mức trình tự không thành vấn đề. Tuy nhiên, trong những năm 1970, dường như bất kỳ dạng mã hóa mạnh nào cũng luôn phải tuân thủ quy tắc "vào sau ra trước". Nếu một bức thư được mã hóa bằng chìa khóa mã của Alice rồi sau đó bằng chìa

khóa mã của Bob thì nó phải được giải mã bằng chìa khóa mã của Bob trước khi được giải mã bằng chìa khóa mã của Alice. Trình tự quan trọng ngay cả đối với mật mã thay thế dùng một bảng chữ cái. Hãy hình dung Alice và Bob đều có chìa khóa mã riêng, như trình bày dưới đây, và chúng ta hãy xem điều gì xảy ra nếu trình tự được thực hiện không đúng. Alice sử dụng chìa khóa mã để mã hóa một bức thư gửi cho Bob, sau đó Bob mã hóa tiếp bằng chìa khóa mã của anh ta; Alice giải mã phần của mình nhờ chìa khóa mã riêng và cuối cùng Bob sử dụng chìa khóa mã của mình để giải mã toàn bộ.

Chìa khóa mã của Alice

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Chìa khóa mã của Bob

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Thư *(Gặp em vào buổi trưa)*

	m	e	e	t		m	e		a	t		n	o	o	n
Mã hóa bằng chìa khóa mã của Alice	Y	G	G	C		Y	G		H	C		J	B	B	J
Mã hóa bằng chìa khóa mã của Bob	L	N	N	M		L	N		O	M		E	P	P	E
Mã hóa bằng chìa khóa mã của Alice	Z	Q	Q	X		Z	Q		L	X		K	P	P	K
Mã hóa bằng chìa khóa mã của Bob	w	n	n	t		w	n		y	t		x	b	b	x

Kết quả nhận được là vô nghĩa. Tuy nhiên, bạn có thể tự kiểm tra đối với trình tự giải mã ngược lại, cụ thể là Bob giải mã trước Alice, tức là tuân thủ quy tắc "vào sau ra trước", thì kết quả sẽ lại là bức thư ban đầu. Song nếu trình tự là quan trọng như vậy

thì tại sao hệ thống khóa móc lại có kết quả trong giai thoại về các hộp có khóa? Câu trả lời là trình tự không quan trọng với khóa móc. Tôi có thể sử dụng 20 khóa móc vào một hộp và mở chúng theo bất kỳ trình tự nào thì cuối cùng cái hộp cũng sẽ mở ra được. Tiếc thay là hệ thống mã hóa lại nhạy cảm hơn nhiều đối với trình tự.

Mặc dù cách tiếp cận hộp khóa kép không ứng dụng được cho khoa mật mã trong thế giới thực, song nó vẫn gây cảm hứng cho Diffie và Hellman tìm kiếm một phương pháp thực tế để giải quyết khôn khéo vấn đề phân phối chìa khóa mã. Họ miệt mài hết tháng này đến tháng khác cố gắng tìm ra một giải pháp. Mặc dù mỗi ý tưởng đều kết thúc thất bại, song họ xử sự như những thằng ngốc lý tưởng và hết sức kiên trì. Nghiên cứu của họ tập trung xem xét các *hàm số* toán học khác nhau. Hàm số là phép toán nào đó biến một số này thành một số khác. Ví dụ, "nhân đôi" là một dạng hàm số, vì nó biến số 3 thành 6, hay số 9 thành 18. Hơn nữa, chúng ta cũng có thể cho rằng tất cả các dạng mã hóa bằng máy tính cũng là các hàm số vì chúng biến một số (văn bản thường) thành một số khác (văn bản mật mã).

Hầu hết các hàm số toán học được phân loại là các hàm số hai chiều vì chúng dễ thực hiện và dễ làm ngược lại. Ví dụ, "nhân đôi" là một hàm số hai chiều vì dễ dàng nhân đôi một số để tạo thành một số mới, và cũng dễ dàng làm hàm số ngược lại, tức là chuyển số gấp đôi trở về số ban đầu. Chẳng hạn, nếu chúng ta biết kết quả gấp đôi là 26 thì sẽ không khó khăn khi đảo ngược hàm và suy ra số ban đầu là 13. Cách đơn giản nhất để hiểu về khái niệm hàm hai chiều là xét một hành động hằng ngày. Động tác bật công tắc đèn là một hàm số, vì nó biến một bóng đèn bình

thường thành một bóng đèn phát sáng. Hàm số này là hai chiều vì nếu một công tắc được bật lên thì cũng dễ dàng tắt nó đi và biến bóng đèn trở về trạng thái ban đầu.

Tuy nhiên Diffie và Hellman không quan tâm đến các hàm số hai chiều. Họ tập trung sự chú ý của mình đến các hàm số một chiều. Như tên gọi của chúng gợi ý, hàm số một chiều là dễ dàng thực hiện song rất khó để đảo ngược lại. Nói cách khác, hàm số hai chiều là có thể đảo ngược còn hàm một chiều là không thể đảo ngược. Một lần nữa, cách minh họa tốt nhất về hàm một chiều là xét một hành động hằng ngày. Trộn sơn màu vàng và màu xanh da trời để tạo ra sơn màu xanh lá cây là một hàm một chiều, vì rất dễ dàng trộn sơn vào với nhau song lại không thể tách chúng ra khỏi nhau. Một hàm số một chiều khác đó là đánh vỡ một quả trứng, rất dễ làm vỡ trứng song lại không thể biến nó trở lại thành quả trứng nguyên vẹn như ban đầu. Với lý do này, hàm số một chiều đôi khi còn được gọi là các hàm Humpty Dumpty*.

Số học môđun hay *số học đồng dư*, đôi khi còn gọi là *số học đồng hồ*, là một lĩnh vực toán học rất giàu các hàm số một chiều. Trong số học môđun, các nhà toán học xem xét một nhóm hữu hạn các con số được xếp thành vòng tròn, giống như các số trên mặt đồng hồ. Chẳng hạn, Hình 64 trình bày một đồng hồ với

---

* Đây là tên một nhân vật có hình quả trứng trong cuốn truyện nổi tiếng *Alice ở thế giới thần kỳ* của Lewis Carroll. Để hiểu các hàm một chiều tại sao lại được gọi là các hàm số Humpty Dumpty hãy đọc đoạn thơ sau mà Alice đã đọc để chế nhạo Humpty Dumpty:

Ngài Humpty Dumpty ngồi trên bức tường
Ngài Humpty Dumpty bị ngã rất đau
Tất cả ngựa và quân lính của nhà Vua
Cũng không đặt được Ngài về chỗ cũ. (ND)

môđun 7 (hay viết tắt là mod 7), chỉ với bảy con số từ 0 đến 6. Để tính 2 + 3, chúng ta bắt đầu từ số 2 và dịch chuyển theo vòng tròn đi ba vị trí sẽ đạt đến số 5, một kết quả giống như số học thông thường. Để tính 2 + 6, chúng ta bắt đầu từ 2 và dịch chuyển đi sáu vị trí, nhưng lần này chúng ta đi quanh vòng tròn và đến vị trí số 1, không giống với kết quả mà chúng ta thu được trong số học thông thường. Kết quả này được biểu thị như sau:

$2 + 3 = 5 \pmod 7$ và $2 + 6 = 1 \pmod 7$.

Số học môđun tương đối đơn giản, và trong thực tế chúng ta dùng nó hằng ngày khi nói về thời gian. Nếu hiện tại là 9 giờ, chúng ta có cuộc gặp sau 8 tiếng nữa, chúng ta thường nói là sẽ gặp nhau vào lúc 5 giờ, chứ không nói là 17 giờ. Ở đây chúng ta đã tính nhẩm 9 + 8 theo (mod 12). Hãy tưởng tượng ra mặt đồng hồ, nhìn vào số 9 sau đó dịch chuyển theo vòng tròn 8 vị trí và kết thúc tại 5:

$9 + 8 = 5 \pmod{12}$

Thay vì nhìn vào đồng hồ, các nhà toán học thường làm tắt việc tính toán các môđun theo cách sau. Trước hết, thực hiện phép tính trong số học thông thường. Sau đó, nếu chúng ta muốn biết kết quả theo (môđun x), chúng ta chia kết quả thông thường cho x và ghi lại số dư. Số dư này chính là kết quả theo (mod x). Để tính $11 \times 9 \pmod{13}$, chúng ta làm như sau:

$11 \times 9 = 99$

99: 13 = 7, dư 8

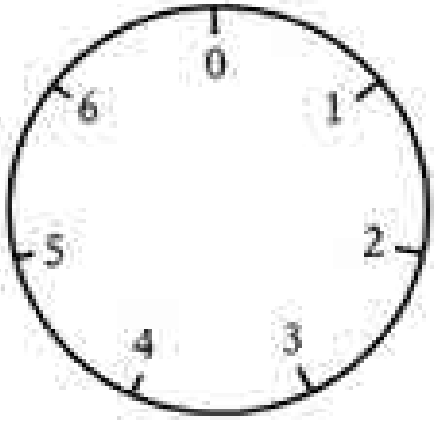
$11 \times 9 = 8 \pmod{13}$

Các hàm số thực hiện trong môi trường số học môđun đều có xu hướng hành xử một cách thất thường, vì vậy đôi khi biến

chúng thành các hàm số một chiều. Điều này trở nên rõ ràng khi so sánh một hàm số đơn giản trong số học thông thường với cùng hàm số đó trong số học môđun. Trong môi trường thứ nhất, hàm số sẽ là hai chiều và dễ đảo ngược; trong môi trường thứ hai, nó sẽ là một chiều và khó đảo ngược. Chúng ta hãy lấy ví dụ như hàm 3^x, chẳng hạn. Tức là lấy một số x rồi nhân 3 với chính nó x lần để đạt được một số mới. Chẳng hạn, nếu $x = 2$ và chúng ta thực hiện hàm số đó, thì:

$$3^x = 3^2 = 3 \times 3 = 9$$

Nói cách khác, hàm số này biến số 2 thành số 9. Trong số học thông thường, khi giá trị của x tăng thì kết quả của hàm số cũng tăng. Do đó, nếu chúng ta được cho trước kết quả của hàm thì sẽ khá dễ dàng tính ngược lại và suy ra số ban đầu. Ví dụ, nếu kết quả là 81, chúng ta có thể suy ra $x = 4$ vì $3^4 = 81$. Nếu chúng ta nhầm lẫn và đoán $x = 5$ thì có thể tính ra $3^5=243$, cho thấy sự lựa chọn của chúng ta về giá trị của x là quá lớn. Sau đó, chúng ta giảm giá trị lựa chọn của x xuống 4, và khi đó sẽ thu được kết quả đúng. Tóm lại, ngay cả khi chúng ta đoán sai, chúng ta vẫn có thể tìm đúng giá trị của x, và nhờ đó mà đảo ngược được hàm số.



Hình 64. Số học môđun được thực hiện trên một tập hợp số hữu hạn, có thể coi như các số trên mặt đồng hồ. Trong trường hợp này, chúng ta có thể tính 6 + 5 theo môđun 7 bằng cách nhìn vào số 6 và dịch chuyển theo vòng tròn đi năm vị trí, ta sẽ nhận được kết quả là 4.

Tuy nhiên, trong số học môđun, hàm số này không hành xử một cách hợp lý như vậy. Hãy tưởng tượng rằng người ta cho chúng ta biết giá trị của 3^x theo (mod 7) là 1, và yêu cầu tìm giá trị của x. Không giá trị nào lấp ló trong đầu vì chúng ta nhìn chung là không quen với số học môđun. Ta có thể đoán là $x = 5$ và tính ra kết quả của 3^5(mod 7). Kết quả tính được là 5, quá lớn, vì kết quả mong đợi là 1. Chúng ta thử giảm giá trị của x và thử lần nữa. Nhưng làm như vậy là sai hướng vì giá trị thực của x là bằng 6.

Trong số học thông thường, chúng ta có thể thử các số và có thể cảm giác được chúng ta đang "ấm" lên hay "lạnh" đi. Song môi trường số học môđun lại chẳng cho ta những đầu mối hữu ích nào và do đó việc đảo ngược hàm số khó hơn rất nhiều. Thường chỉ có một cách đảo ngược hàm trong số học môđun, đó là lập một bảng tính toán giá trị của hàm tại nhiều giá trị của x cho đến khi tìm thấy kết quả đúng. Bảng 25 trình bày kết quả tính một số giá trị của hàm trong cả số học thông thường lẫn số học môđun. Nó minh họa một cách rõ ràng hành vi thất thường của hàm số khi được tính trong số học môđun. Mặc dù lập ra một bảng như vậy chỉ là việc làm tẻ ngắt khi tính toán với các số tương đối nhỏ, song sẽ là rất khổ nhọc nếu phải lập một bảng với hàm số như 453^x (mod 21.997). Đây là một ví dụ kinh điển về hàm một chiều, vì tôi có thể lấy một giá trị của x và tính toán ra kết quả của hàm, song nếu tôi đưa cho bạn một kết quả, giả sử là 5.787 thì bạn sẽ cực kỳ khó khăn để đảo ngược hàm và suy ra giá trị của x. Sẽ chỉ mất vài giây để tôi tính toán và tìm ra 5.787 song bạn sẽ phải mất hàng giờ để lập bảng và tính ra giá trị của x.

Bảng 25. Giá trị của hàm 3^x được tính trong số học thông thường (dòng thứ hai) và số học môđun (dòng thứ ba). Hàm số tăng lên liên tục ở số học thông thường song lại rất thất thường trong số học môđun.

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

Sau hai năm tập trung vào số học môđun và hàm số một chiều, sự ngốc nghếch của Hellman bắt đầu được đền đáp. Vào mùa xuân năm 1976, ông đã tìm ra một chiến lược giải quyết được vấn đề trao đổi chìa khóa mã. Trong vòng một tiếng rưỡi đồng hồ viết nguệch ngoạc một cách điên rồ trên bảng, ông đã chứng minh rằng Alice và Bob có thể thống nhất một chìa khóa mã mà không cần gặp nhau, nhờ đó đã đánh bại một chân lý đã tồn tại hàng thế kỷ nay. Ý tưởng của Hellman dựa trên hàm số một chiều có dạng $Y^x \pmod P$. Ban đầu, Alice và Bob thống nhất giá trị của Y và P. Hầu hết mọi giá trị đều có thể chấp nhận, song có một số giới hạn, chẳng hạn như Y phải nhỏ hơn P. Các giá trị này không cần giữ bí mật, nên Alice có thể gọi thẳng cho Bob và đề nghị, chẳng hạn $Y = 7$ và $P = 11$. Ngay cả nếu đường dây điện thoại không an toàn và Eve xấu bụng nghe được cuộc nói chuyện này thì cũng không quan trọng, như sau này chúng ta sẽ thấy. Như vậy, Alice và Bob giờ đã thống nhất hàm số một chiều $7^x \pmod{11}$. Lúc này, họ có thể bắt đầu quá trình thử thiết lập một chìa khóa mã mà không cần gặp nhau. Vì họ làm song song nên tôi giải thích hành động của họ ở hai cột như trên Bảng 26.

Bảng 26. Hàm số một chiều tổng quát là Y^X (mod *P*). Alice và Bob cùng lựa chọn giá trị cho *Y* và *P*, và vì vậy thống nhất được hàm một chiều là 7^X (mod 11).

	Alice	Bob
Bước 1	Alice lựa chọn một số, chẳng hạn như 3 và giữ bí mật số này. Chúng ta ký hiệu số này của Alice là A	Bob lựa chọn một số, chẳng hạn như 6 và giữ bí mật số này. Chúng ta ký hiệu số này của Bob là B
Bước 2	Alice thay 3 vào hàm số một chiều và tính ra kết quả của 7^A (mod 11): 7^3 (mod 11) = 343 (mod 11) = 2	Bob thay 6 vào hàm số một chiều và tính ra kết quả của 7^B (mod 11): 7^6 (mod 11) = 117.649 (mod 11) = 4
Bước 3	Alice gọi kết quả của tính toán này là α và gửi kết quả, tức là 2, cho Bob	Bob gọi kết quả của tính toán này là β và gửi kết quả, tức là 4, cho Alice
Trao đổi	Thông thường đây sẽ là thời điểm quan trọng, vì Alice và Bob đang trao đổi thông tin và vì vậy đây là cơ hội để cho Eva nghe trộm và phát hiện ra các chi tiết của thông tin. Tuy nhiên, hóa ra Eva có thể nghe mà không ảnh hưởng gì đến độ an toàn cuối cùng của hệ thống. Alice và Bob có thể sử dụng cùng đường dây điện thoại như đã sử dụng để thống nhất các giá trị của *Y* và *P*, và Eva có thể nghe được hai số được trao đổi là 2 và 4. Tuy nhiên, các con số này không phải là chìa khóa mã, do vậy sẽ không có vấn đề gì nếu Eva biết được các con số đó.	
Bước 4	Alice dùng kết quả của Bob và tính β^A (mod 11): 4^3 (mod 11) = 64 (mod 11) = 9	Bob dùng kết quả của Alice và tính α^B (mod 11): 2^6 (mod 11) = 64 (mod 11) = 9
Chìa khóa mã	Thật kỳ diệu, Alice và Bob cuối cùng đều kết thúc bằng cùng số, 9. Đó là chìa khóa mã!	

Sau khi thực hiện theo các bước trong Bảng 26, bạn sẽ thấy, không cần gặp nhau, Alice và Bob vẫn thống nhất được một chìa khóa mã mà họ có thể sử dụng để mã hóa thư. Chẳng hạn, họ có thể sử dụng số 9 như là chìa khóa mã cho mã hóa bằng DES. (DES thực sự sử dụng các số lớn hơn nhiều để làm chìa khóa mã và quá trình trao đổi được mô tả trong Bảng 26 sẽ được thực hiện với các số lớn hơn nhiều, tạo ra chìa khóa mã DES cũng lớn hơn). Bằng việc sử dụng cơ chế của Hellman, Alice và Bob đã có thể thống nhất chìa khóa mã, song họ không phải gặp nhau và thì thầm với nhau về chìa khóa mã. Thành công kỳ diệu là chìa khóa mã được thống nhất qua trao đổi trên đường dây điện thoại thông thường. Nhưng nếu Eve nghe trộm được thì liệu có chắc chắn là cô ta sẽ không thể biết được chìa khóa mã không?

Bây giờ chúng ta hãy thử kiểm tra sơ đồ của Hellman theo quan điểm của Eve. Nếu cô ấy nghe lén và biết các thông tin sau: hàm số là $7^x \pmod{11}$, Alice gửi $\alpha = 2$ và Bob gửi $\beta = 4$. Để tìm ra chìa khóa mã, Eve phải làm như Bob, tức là biến α thành chìa khóa mã nhờ đã biết B, hay làm như Alice biến β thành chìa khóa mã nhờ đã biết A. Tuy nhiên, Eve không biết giá trị của A hay B vì Alice và Bob không trao đổi các số này và giữ bí mật chúng. Và Eve rơi vào ngõ cụt. Cô chỉ còn một hy vọng: về lý thuyết, cô có thể tính ra A từ α, vì a là kết quả của việc thay A vào hàm số mà Eve đã biết. Hoặc cô cũng có thể tính B từ β vì β là kết quả của việc thay B vào hàm số mà cô cũng đã biết. Không may cho Eve, hàm số là một chiều nên trong khi Alice dễ dàng biến A thành α và Bob biến B thành β nhưng Eva lại rất khó khăn để đảo ngược lại quá trình đó, đặc biệt là nếu các con số là cực lớn.

Bob và Alice đã trao đổi thông tin đủ để giúp họ thiết lập nên

một chìa khóa mã, song thông tin này lại không đủ với Eve để tính toán ra chìa khóa mã. Cũng tương tự như sơ đồ của Hellman, hãy tưởng tượng một mật mã bằng cách nào đó dùng màu sắc làm chìa khóa mã. Trước hết, chúng ta giả định rằng mọi người, trong đó có cả Alice, Bob và Eve, đều có một lọ dung tích ba lít chứa một lít sơn màu vàng. Nếu Alice và Bob muốn thống nhất chìa khóa mã, mỗi người đổ thêm vào lọ của mình một lít màu bí mật. Alice có thể đổ một ít màu tím trong khi Bob có thể đổ thêm vào màu đỏ sẫm. Mỗi người sau đó gửi lọ hỗn hợp của mình cho nhau. Cuối cùng, Alice đổ thêm vào hỗn hợp của Bob màu bí mật của cô còn Bob đổ vào hỗn hợp của Alice màu bí mật của anh. Cả hai lọ lúc này sẽ có cùng một màu, vì chúng đều có chứa một lít màu vàng, một lít màu tím và một lít màu đỏ sẫm. Đây chính là màu chính xác của cái lọ đã được pha thêm hai lần và được sử dụng làm chìa khóa mã. Alice không biết Bob đã đổ thêm màu gì và Bob cũng vậy, song cuối cùng họ đều thu được cùng một màu. Trong khi đó Eve lại rất bối rối. Ngay cả khi cô bắt được những cái lọ trung gian, cô cũng không thể tìm ra màu của cái lọ cuối cùng, chính là chìa khóa mã đã được thống nhất. Cô có thể nhìn thấy màu của cái lọ hỗn hợp của màu vàng và màu mà Alice đã thêm vào trên đường gửi đến chỗ Bob, và cũng có thể nhìn thấy màu của cái lọ hỗn hợp màu vàng và màu bí mật mà Bob đã thêm vào trên đường gửi đến chỗ Alice, song để tìm ra chìa khóa mã, cô cần phải biết màu bí mật ban đầu của Alice và Bob. Tuy nhiên, Eve không thể tìm ra nếu chỉ nhìn vào lọ hỗn hợp. Ngay cả nếu cô có lấy mẫu từ một trong các màu sơn hỗn hợp, cô cũng không thể tách màu ra để tìm được màu bí mật, vì hỗn hợp sơn là hàm số một chiều.

Đột phá của Hellman nảy ra khi ông làm việc ở nhà một hôm vào đêm khuya, nên lúc ông tính toán xong thì đã quá muộn để gọi điện cho Diffie và Merkle. Ông đã chờ cho đến sáng hôm sau để tiết lộ phát minh của mình cho hai người bạn, hai người duy nhất trên thế giới cũng tin rằng có một giải pháp khả thi đối với vấn đề phân phối chìa khóa mã. "Nàng thơ đã thì thầm riêng với tôi", Hellman kể, "song tất cả chúng tôi đã cùng nhau đặt nền móng". Diffie ngay lập tức nhận ra sức mạnh của phát minh của Hellman: "Marty đã giải thích hệ thống của anh về trao đổi chìa khóa mã với tất cả sự đơn giản đến mức không thể tin nổi của nó. Lắng nghe anh ấy nói, tôi chợt nhận ra ý niệm đó đôi khi cũng đã từng lấp ló trong tâm trí tôi, song nó đã không thực sự bật ra."

Sơ đồ trao đổi chìa khóa mã Diffie-Hellman-Merkle, như được gọi ngày nay, đã giúp Alice và Bob có thể thiết lập một bí mật qua trao đổi công khai. Đó là một trong những khám phá khác thường nhất trong lịch sử khoa học và buộc các cơ quan mật mã phải viết lại các quy tắc mã hóa. Diffie, Hellman và Merkle đã chứng minh công khai những khám phá của họ tại Hội nghị Máy tính Quốc gia vào tháng Sáu năm 1976, và đã làm cho cử tọa là các chuyên gia mật mã phải kinh ngạc. Một năm sau, họ đã được nhận bằng phát minh sáng chế. Từ nay, Alice và Bob không phải gặp nhau để trao đổi chìa khóa mã nữa. Thay vào đó, Alice có thể gọi cho Bob trên điện thoại, trao đổi một cặp số với Bob, rồi cùng nhau thiết lập một chìa khóa mã và sau đó tiến hành mã hóa.

Tuy trao đổi chìa khóa mã Diffie-Hellman-Merkle là một bước nhảy vượt bậc, song hệ thống vẫn chưa hoàn hảo vì vẫn còn có những bất tiện. Hãy tưởng tượng rằng Alice sống ở Hawaii, và

cô muốn gửi thư điện tử cho Bob ở Instanbul. Bob có thể đang ngủ, song điểm thú vị của e-mail, đó là Alice có thể gửi thư vào bất cứ lúc nào và nó vẫn đợi trên máy tính của Bob khi anh tỉnh giấc. Tuy nhiên, nếu Alice muốn mã hóa thư của mình thì cô phải thống nhất chìa khóa mã với Bob, và để tiến hành trao đổi thì thích hợp nhất là Alice và Bob phải cùng trên mạng, vì thiết lập một chìa khóa mã đòi hỏi sự trao đổi thông tin hai chiều. Muốn vậy, Alice phải đợi Bob thức dậy. Một cách khác, Alice có thể chuyển phần của mình trước rồi đợi trả lời của Bob sau 12 tiếng, lúc ấy chìa khóa sẽ được thiết lập và Alice có thể, nếu cô chưa ngủ, mã hóa và gửi thư đi. Dù theo cách nào thì hệ thống trao đổi chìa khóa mã của Hellman vẫn làm chậm tính tức thời của thư điện tử.

Như vậy, Hellman đã làm tiêu tan một trong những giáo lý của khoa mật mã và chứng minh được rằng Bob và Alice không phải gặp nhau để thống nhất chìa khóa mã. Tiếp theo, chỉ cần một ai khác tìm ra một sơ đồ hiệu quả hơn là vấn đề phân phối chìa khóa mã sẽ được giải quyết một cách trọn vẹn.

Sự ra đời của Mật mã chìa khóa công khai

Mary Fisher không bao giờ quên lần đầu tiên Whitfield Diffie hẹn hò bà: "Ông ấy biết tôi yêu thích không gian nên đã mời tôi đi chơi và ăn trưa. Whit giải thích rằng tối hôm ấy ông sẽ đi xem Skylab (Phòng thí nghiệm không gian) cất cánh, và vì vậy chúng tôi đã lái xe suốt đêm và tới đó lúc 3 giờ sáng. Con chim đã ở trên đường, như họ vẫn thường nói hồi đó. Whit có những thành tích nổi bật chứ tôi thì không. Vì vậy, khi họ hỏi thẻ căn cước của

tôi và hỏi tôi là ai, Whit nói 'Vợ tôi'. Đó là ngày 16 tháng Mười một năm 1973". Họ cuối cùng đã lấy nhau, và trong suốt những năm đầu, Mary đã giúp đỡ ông trong những lúc ông mải mê suy tư về mật mã. Lúc đó Diffie vẫn còn là nghiên cứu sinh nên ông chỉ nhận được đồng lương ít ỏi. Còn Mary, một nhà khảo cổ học được đào tạo bài bản, đã kiếm được việc làm ở Công ty Dầu mỏ Anh quốc nên cũng tùng tiệm đủ sống.

Trong khi Martin Hellman đang nghiên cứu phương pháp trao đổi chìa khóa mã của mình thì Whitfield Diffie lại thực hiện một cách tiếp cận hoàn toàn khác để giải quyết vấn đề phân phối chìa khóa mã. Ông thường mất những khoảng thời gian dài tập trung suy nghĩ nhưng không mang lại kết quả. Và một lần vào năm 1975, ông đã thất vọng đến mức buột miệng bảo với Mary rằng ông là một nhà khoa học thất bại, chẳng bao giờ làm nên trò trống gì. Ông thậm chí còn bảo bà nên tìm một người đàn ông khác. Mary đã nói với ông rằng bà có một niềm tin tuyệt đối vào ông và chỉ hai tuần sau Diffie đã nảy ra một ý tưởng thực sự sáng chói.

Ông vẫn nhớ được ý tưởng đó đã lóe lên trong óc ông như thế nào và sau đó thì hầu như biến mất: "Tôi đi xuống tầng dưới để lấy một lon Coke và gần như đã quên biến ý tưởng đó. Tôi nhớ rằng mình đang nghĩ về một điều gì đó rất lý thú, song không thể nhớ lại được nó là cái gì. Rồi, nó bỗng trở lại trong sự phấn khích dâng trào thực sự. Tôi nhận ra rằng lần đầu tiên tôi đã khám phá ra một cái gì đó thực sự có giá trị trong sự nghiệp nghiên cứu mật mã của mình. Mọi thứ mà tôi đã khám phá trong lĩnh vực này từ trước tới nay đối với tôi dường như chỉ là những chi tiết kỹ thuật không mấy quan trọng". Lúc đó là vào khoảng giữa buổi chiều và

ông phải đợi vài giờ sau Mary mới trở về. "Whit đang đứng đợi trước cửa", bà nhớ lại. "Ông ấy bảo có một chuyện muốn nói với tôi và trên mặt ông ấy có vẻ gì đó rất buồn cười. Tôi bước vào và ông ấy nói, 'Ngồi xuống đi em, anh muốn nói chuyện với em. Anh tin rằng mình đã có một khám phá vĩ đại - Anh biết anh là người đầu tiên làm được việc này'. Thế giới dường như ngưng lại với tôi giây phút đó. Tôi cảm thấy như mình đang sống trong một bộ phim của Hollywood."

Diffie đã tạo ra một loại mật mã mới, kết hợp chặt chẽ với cái được gọi là *chìa khóa mã bất đối xứng*. Cho đến đây, tất cả các kỹ thuật mã hóa mô tả trong cuốn sách này đều là *đối xứng*, tức là quá trình giải mã chỉ đơn giản là làm ngược lại với quá trình mã hóa. Chẳng hạn, máy Enigma sử dụng cách cài đặt chìa khóa mã nhất định để mã hóa thông tin và người nhận sử dụng một cái máy giống hệt với cùng một cách cài đặt chìa khóa mã. Tương tự như vậy, mã hóa DES sử dụng một chìa khóa mã để thực hiện 16 vòng mã hóa, và sau đó việc giải mã DES cũng sử dụng cùng chìa khóa mã để thực hiện 16 vòng đảo ngược lại. Cả người gửi và người nhận đều có sự hiểu biết tương đương nhau, và họ đều sử dụng cùng một chìa khóa mã để mã hóa và giải mã, tức mối quan hệ giữa họ là đối xứng. Trái lại, trong một hệ thống chìa khóa mã bất đối xứng, chìa khóa để mã hóa và chìa khóa để giải mã không giống hệt như nhau, đúng như cái tên của nó cho thấy. Trong mật mã bất đối xứng, nếu Alice biết chìa khóa để mã hóa, cô ấy có thể mã hóa thư, song cô ấy không thể giải mã được bức thư đó. Để giải mã, Alice phải có được chìa khóa giải mã. Sự khác biệt giữa chìa khóa để mã hóa và giải mã chính là điểm khiến cho mật mã bất đối xứng trở nên đặc biệt.

Đến đây cũng cần nhấn mạnh rằng Diffie mới chỉ tìm ra khái niệm chung về một mật mã bất đối xứng, chứ chưa thực sự tạo ra một ví dụ mật mã cụ thể nào. Tuy nhiên, chỉ riêng khái niệm về một mật mã bất đối xứng thôi cũng đã là một cuộc cách mạng. Nếu các nhà tạo mã có thể tìm ra một mật mã bất đối xứng thực sự, một hệ thống thỏa mãn các yêu cầu của Diffie, thì những hệ quả của nó đối với Alice và Bob sẽ là cực kỳ to lớn. Alice có thể tạo ra các cặp chìa khóa của riêng mình: chìa khóa mã hóa và chìa khóa giải mã. Nếu chúng ta giả sử rằng mật mã bất đối xứng là một dạng mật mã máy tính thì chìa khóa mã hóa của Alice sẽ là một con số, và chìa khóa giải mã là một con số khác. Alice giữ bí mật chìa khóa giải mã, vì vậy thường thì nó được gọi là *chìa khóa riêng* của Alice. Tuy nhiên, cô ấy lại công khai chìa khóa mã hóa và ai cũng có thể có nó, vì vậy nó thường được gọi là *chìa khóa công khai* của Alice. Nếu Bob muốn gửi cho Alice một bức thư, anh đơn giản chỉ cần tìm chìa khóa mã công khai của cô ấy trong một danh sách tương tự như danh bạ điện thoại. Sau đó, Bob sử dụng chìa khóa mã công khai của Alice để mã hóa thư. Anh gửi bức thư mã hóa cho Alice và sau khi bức thư đến nơi, Alice có thể giải mã nó bằng chìa khóa giải mã riêng của mình. Tương tự, nếu Charlie, Dawn, hay Edward muốn gửi thư được mã hóa cho Alice, họ cũng có thể tìm chìa khóa công khai của Alice và trong mỗi trường hợp, chỉ có mình Alice là có chìa khóa giải mã riêng để giải mã các bức thư đó.

Lợi thế to lớn của hệ thống này, đó là nó không cần có sự đi-lại như khi trao đổi chìa khóa mã Diffie-Hellman-Merkle. Bob không phải đợi nhận được thông tin từ Alice trước khi mã hóa và gửi thư cho cô, anh ta chỉ cần tìm chìa khóa mã hóa công khai

của Alice mà thôi. Hơn nữa, mật mã bất đối xứng cũng vẫn giải quyết được vấn đề phân phối chìa khóa mã. Alice không phải chuyển chìa khóa mã công khai của mình một cách bí mật cho Bob, mà hoàn toàn ngược lại, bây giờ cô có thể công khai chìa khóa mã hóa của mình rộng rãi đến đâu cũng được. Thậm chí cô có thể cho cả thế giới biết chìa khóa mã công khai của mình để mọi người đều có thể sử dụng nó để gửi thư bí mật cho cô. Đồng thời, ngay cả nếu toàn thế giới biết chìa khóa công khai của Alice thì cũng không có ai trong số họ, kể cả Eve, có thể giải mã được bất kỳ bức thư đã được mã hóa nào bằng chìa khóa đó, vì việc biết chìa khóa công khai không giúp ích gì cho việc giải mã hết. Thực tế, một khi Bob đã mã hóa thư bằng chìa khóa công khai của Alice thì ngay cả anh cũng không thể giải mã nổi. Chỉ Alice, người sở hữu chìa khóa mã riêng mới có thể giải mã được bức thư đó.

Điều này hoàn toàn ngược lại với mật mã đối xứng truyền thống, trong đó Alice phải đi một chặng đường dài để chuyển chìa khóa mã một cách an toàn đến cho Bob. Trong mật mã đối xứng, chìa khóa mã hóa cũng chính là chìa khóa giải mã, nên Alice và Bob phải cực kỳ thận trọng để đảm bảo rằng chìa khóa này không bị rơi vào tay Eve. Đây chính là cái gốc của vấn đề phân phối chìa khóa mã.

Trở lại sự tương tự với các khóa móc, thì mật mã bất đối xứng có thể được hình dung như sau. Bất kỳ ai cũng có thể khóa một chiếc khóa móc một cách đơn giản là bấm nó vào, nhưng chỉ người có chìa khóa mới có thể mở được nó. Khóa (mã hóa) thì dễ, một điều mà ai cũng có thể làm được, song mở (giải mã) thì chỉ có thể thực hiện được bởi người sở hữu chìa khóa. Việc biết

bấm chiếc khóa móc tầm thường không cho bạn biết làm thế nào để mở nó. Nói rộng ra, hãy tưởng tượng Alice thiết kế một khóa móc và chìa khóa của nó. Cô ấy giữ chìa khóa song cho sản xuất hàng ngàn khóa móc giống hệt nhau và gửi chúng đi khắp thế giới qua bưu điện. Nếu Bob muốn gửi một bức thư, anh cho nó vào một cái hộp, đến bưu điện địa phương và yêu cầu một "khóa móc Alice" rồi khóa hộp lại. Giờ thì anh không thể mở được hộp nữa, nhưng khi Alice nhận được, cô ấy có thể mở nó bằng chiếc chìa khóa duy nhất. Khóa móc và quá trình bấm khóa là tương đương với chìa khóa mã hóa công khai, vì mọi người đều có thể có được khóa móc, và ai cũng có thể sử dụng khóa móc để niêm phong thư trong hộp. Chìa khóa của khóa móc tương đương với chìa khóa giải mã riêng, vì chỉ Alice mới có nó, chỉ cô mới mở được khóa và chỉ cô mới lấy được lá thư trong hộp ra.

Hệ thống có vẻ như đơn giản khi được giải thích nhờ sự tương tự với các khóa móc, song việc tìm ra một hàm số toán học thực hiện được điều tương tự lại không hề tầm thường, khi kết hợp nó vào một hệ thống mật mã khả thi. Để đưa mật mã bất đối xứng từ một ý tưởng lớn thành một phát minh dùng được trong thực tế thì phải có ai đó tìm ra một hàm số toán học thích hợp. Diffie đã nghiên cứu một loại hàm số một chiều đặc biệt, một hàm số có thể đảo ngược được trong những điều kiện ngoại lệ. Trong hệ thống bất đối xứng của Diffie, Bob mã hóa bức thư bằng chìa khóa công khai, song anh không thể giải mã được nó - đây thực sự chính là hàm số một chiều. Tuy nhiên, Alice có thể giải mã được bức thư vì cô có chìa khóa riêng, đó là một ít thông tin đặc biệt giúp cô đảo ngược được hàm số này. Một lần nữa, khóa móc lại là một sự tương tự hữu ích - bấm khóa móc vào là một

hàm số một chiều, vì nói chung là khó mở ra nếu không có gì đó đặc biệt (chìa khóa riêng), nhưng nếu có nó, hàm số lại được đảo ngược dễ dàng.

Diffie đã cho công bố một bài báo trình bày khái quát ý tưởng của mình vào mùa hè năm 1975, rồi sau đó các nhà khoa học khác đã tham gia nghiên cứu nhằm tìm kiếm một hàm số một chiều thích hợp, tức là một hàm số thỏa mãn những điều kiện mà một mật mã bất đối xứng đòi hỏi. Ban đầu ai nấy đều rất lạc quan, song cho đến cuối năm đó, vẫn chẳng ai tìm ra một hàm số nào thích hợp. Nhiều tháng trôi qua, dường như ngày càng chắc chắn rằng hàm số một chiều đặc biệt đó không tồn tại. Dường như ý tưởng của Diffie chỉ thực hiện trên lý thuyết mà không tồn tại trong thực tế. Nhưng dù sao, đến cuối năm 1976, nhóm của Diffie, Hellman và Merkle cũng đã làm được một cuộc cách mạng trong thế giới mật mã. Họ đã thuyết phục phần còn lại của thế giới rằng có một giải pháp cho vấn đề phân phối chìa khóa mã, và đã tạo ra cái gọi là trao đổi chìa khóa mã Diffie-Hellman-Merkle - một hệ thống vận hành được nhưng chưa hoàn hảo. Họ cũng đã đưa ra khái niệm về mật mã bất đối xứng - một hệ thống hoàn hảo nhưng chưa vận hành được. Họ tiếp tục những nghiên cứu của mình tại Đại học Stanford, cố gắng tìm ra một hàm số một chiều đặc biệt khiến mật mã bất đối xứng trở thành hiện thực. Tuy nhiên, họ đã thất bại. Chiến thắng trong cuộc chạy đua tìm kiếm mật mã bất đối xứng lại thuộc về một bộ ba nghiên cứu khác, cách Bờ Đông nước Mỹ 5.000km.

Các số nguyên tố bước ra sân khấu

"Tôi bước vào văn phòng của Ron Rivest", Leonard Adleman nhớ lại, "và Ron đang cầm bài báo đó trong tay. Anh ấy bắt đầu nói: 'Mấy gã Stanford này đúng là ba láp quá'. Và tôi nhớ mình đã nghĩ 'Tuyệt lắm, Ron, nhưng tôi có chuyện khác muốn nói với anh đây'. Tôi hoàn toàn không hay biết gì về lịch sử khoa học mật mã và tôi cũng chẳng hứng thú gì với những điều anh ấy đang nói". Bài báo khiến Ron Rivest kích động đến như vậy là của Diffie và Hellman, trong đó mô tả khái niệm mật mã bất đối xứng. Cuối cùng, Rivest cũng thuyết phục được Adleman rằng có thể có những điều thú vị về toán học trong vấn đề này và họ đã cùng nhau giải quyết để cố tìm ra một hàm số một chiều thỏa mãn những yêu cầu của một mật mã bất đối xứng. Trong cuộc săn tìm này, họ đã hợp tác với Adi Shamir. Cả ba đều là các nhà nghiên cứu làm việc trên tầng tám của Phòng Thí nghiệm về Khoa học máy tính của MIT.

Rivest, Shamir và Adleman đã hình thành nên một nhóm hoàn hảo. Rivest là một nhà khoa học về máy tính với khả năng hấp thu những ý tưởng mới rất khác thường và ứng dụng chúng vào những chỗ không chắc thành công. Ông luôn theo dõi sát những bài báo khoa học mới nhất, chính chúng đã tạo cho ông cảm hứng tìm ra một loạt những ứng viên kỳ lạ và tuyệt vời cho hàm số một chiều là trung tâm của mật mã bất đối xứng. Tuy nhiên, mỗi ứng viên lại có những thiếu sót khác nhau. Shamir, một nhà khoa học máy tính khác, lại có một trí tuệ sắc sảo và một khả năng nhìn xuyên thấu những thứ vụn vặt để tập trung vào cốt lõi của vấn đề. Ông cũng thường nghĩ ra những ý tưởng về tạo mật mã bất đối xứng, song những ý tưởng của ông cuối cùng vẫn có những

sơ hở. Adleman, một nhà toán học với khả năng chịu đựng cực lớn, chặt chẽ và kiên nhẫn, người có trách nhiệm rất lớn là phát hiện ra những sai sót trong các ý tưởng của Rivest và Shamir, bảo đảm rằng họ không lãng phí thời gian theo đuổi những phương hướng sai lầm. Rivest và Shamir mất một năm theo đuổi những ý tưởng mới, và Adleman mất một năm để hạ gục chúng. Cả ba người phần nào đã bắt đầu mất hy vọng, song họ không nhận ra rằng quá trình thất bại liên tiếp đó là một phần tất yếu trong nghiên cứu của họ, nó đã dần dần lái họ rời xa lãnh địa toán học khô cằn và hướng đến một vùng đất màu mỡ hơn. Trong quá trình đó, những nỗ lực của họ đã được đền bù.

Vào tháng Tư năm 1977, Rivest, Shamir và Adleman nghỉ lễ Quá Hải* tại nhà của một sinh viên và uống khá nhiều rượu Manischewitz**. Mãi nửa đêm họ mới trở về nhà. Rivest, không ngủ được, vừa nằm trên đivăng vừa đọc một cuốn sách giáo khoa toán. Rồi ông chuyển sang suy ngẫm về câu hỏi đã khiến ông trăn trở hàng tuần lễ - liệu có thể tạo được một mật mã bất đối xứng hay không? Có thể tìm ra một hàm số một chiều mà có thể đảo ngược được chỉ khi người nhận có những thông tin nào đó đặc biệt không? Bất chợt màn sương mù tan dần và ông đã có một phát hiện. Thời gian còn lại của đêm đó, ông định hình ý tưởng của mình, và viết ngay một bài báo khoa học hoàn chỉnh trước khi trời sáng. Rivest đã có một đột phá, song nó chỉ nảy sinh sau suốt một năm hợp tác với Shamir và Adleman, và nó sẽ không thể có được nếu thiếu sự cộng tác của họ. Rivest đã

* Lễ kỷ niệm việc người Do Thái rời khỏi Ai Cập. (ND)

** Rượu làm từ nho và được ướp lạnh, uống vào dịp lễ của người Do Thái. (ND)

kết thúc bài báo với tên tác giả được viết theo vần abc: Adleman, Rivest, Shamir.

Sáng hôm sau, Rivest đưa bài báo cho Adleman, người đã quen với việc thường xuyên phải xé chúng đi, nhưng lần này, ông đã không tìm thấy một lỗi nào. Ông chỉ phê phán về tên tác giả. "Tôi đã bảo Ron bỏ tên tôi ra khỏi bài báo", Adleman nhớ lại, "Tôi nói với anh ấy rằng đấy là phát minh của anh, không phải của tôi. Nhưng Ron từ chối và chúng tôi đã thảo luận về chuyện đó. Chúng tôi đã thỏa thuận rằng tôi sẽ về nhà và suy nghĩ một đêm về điều đó, và cân nhắc xem tôi muốn làm gì. Tôi trở lại ngày hôm sau và đề nghị Ron rằng tôi là tác giả thứ ba. Tôi nhớ lúc đó mình đã nghĩ rằng đó là bài báo ít thú vị nhất mà tôi đã từng đứng tên." Adleman không thể sai lầm hơn thế. Hệ thống, được gọi là RSA (Rivest, Shamir, Adleman) đảo ngược của ARS, đã trở thành mật mã có ảnh hưởng lớn nhất trong khoa học mật mã hiện đại.

Trước khi xem xét ý tưởng của Rivest, dưới đây tôi xin nhắc lại ngắn gọn điều mà các nhà khoa học tìm kiếm nhằm tạo ra mật mã bất đối xứng:

(1) Alice phải tạo một chìa khóa công khai mà sau đó cô sẽ công bố rộng rãi nên Bob (và mọi người khác) có thể sử dụng nó để mã hóa thư gửi cho cô. Vì chìa khóa công khai là hàm số một chiều nên hầu như không ai có thể đảo ngược được nó và giải mã được các bức thư của Alice.

(2) Tuy nhiên, Alice cần phải giải mã được những bức thư gửi đến cho cô. Vì vậy, cô phải có một chìa khóa riêng, tức một mẩu thông tin đặc biệt nào đó cho phép cô đảo ngược được tác dụng của chìa khóa mã công khai. Nhờ vậy, Alice (và chỉ Alice) mới có khả năng giải mã bất kỳ bức thư nào gửi tới cho cô.

Hình 65. Ronald Rivest, Adi Shamir, Leonard Adleman

Cốt lõi của mật mã bất đối xứng của Rivest là một hàm một chiều dựa trên loại các hàm môđun như đã trình bày ở đầu chương. Hàm một chiều của Rivest có thể được sử dụng để mã hóa thư - thư ở đây thực chất chỉ là một số, được nạp vào hàm, và kết quả nhận được chính là văn bản mật mã, cũng là một con số. Tôi sẽ không mô tả chi tiết hàm số một chiều của Rivest ở đây (xin xem Phụ lục J), song tôi sẽ giải thích một khía cạnh đặc biệt của nó, được gọi đơn giản là *N*, vì chính *N* làm cho hàm số một chiều có thể đảo ngược được dưới những điều kiện nhất định, và vì vậy là rất lý tưởng để sử dụng như một mật mã bất đối xứng.

N rất quan trọng vì nó là thành phần linh hoạt trong hàm số một chiều, tức là mỗi người có thể chọn một giá trị riêng cho *N*, và tạo ra hàm số một chiều riêng. Để chọn giá trị của *N* riêng cho mình, Alice lấy hai số nguyên tố, *p* và *q*, và nhân chúng với nhau. Một số nguyên tố là số chỉ chia hết cho 1 và chính nó. Chẳng hạn, 7 là số nguyên tố vì 7 chỉ chia hết cho 1 và 7. Tương tự, 13 là số nguyên tố vì nó chỉ chia hết cho 1 và 13. Tuy nhiên, 8 không phải là số nguyên tố vì nó chia hết cho cả 2 và 4.

Chẳng hạn, Alice có thể chọn số nguyên tố của mình là p = 17.159 và q = 10.247. Nhân hai số này với nhau ta được N=17.159 ×10.247 = 175.828.273. Lựa chọn N của Alice chính là chìa khóa mã hóa công khai, và cô có thể in vào danh thiếp, thông báo trên Internet, hoặc đưa vào một danh bạ chìa khóa mã công khai cùng với các giá trị N của những người khác. Nếu Bob muốn mã hóa thư gửi cho Alice, anh tìm giá trị N (175.828.273) của Alice và sau đó thay vào công thức chung của hàm một chiều, hàm này cũng được thông báo công khai. Giờ Bob có hàm một chiều tạo bởi chìa khóa công khai của Alice, được gọi là hàm số một chiều của Alice. Để mã hóa thư gửi Alice, anh lấy hàm một chiều của Alice, nạp thư vào và ghi lại kết quả rồi gửi cho Alice.

Lúc này, bức thư mã hóa là an toàn vì không ai có thể giải mã được nó. Thư đã được mã hóa với hàm số một chiều nên đảo ngược hàm một chiều và giải mã thư, theo định nghĩa, là rất khó khăn. Tuy nhiên, còn một vấn đề là - làm thế nào Alice giải mã được thư? Để đọc thư gửi đến cho mình, Alice phải có một cách đảo ngược hàm một chiều. Cô cần có được chút ít thông tin đặc biệt nào đó cho phép cô giải mã thư. May mắn cho Alice là Rivest đã thiết lập hàm số một chiều sao cho có thể đảo ngược được nếu ai đó biết được giá trị của p và q, hai số nguyên tố mà tích của chúng cho giá trị N. Mặc dù Alice đã thông báo cho cả thế giới biết về giá trị N là 175.828.273, song cô không tiết lộ các giá trị của p và q, vì vậy chỉ mình cô có thông tin đặc biệt cần thiết để giải mã các bức thư của mình.

Chúng ta có thể hiểu rằng N là chìa khóa công khai, một thông tin sẵn có cho tất cả mọi người và cần thiết để mã hóa thư gửi

cho Alice. Trong khi đó, p và q là chìa khóa riêng, chỉ dành riêng cho Alice, tức là thông tin cần thiết để giải mã thư.

Các chi tiết chính xác về việc sử dụng p và q như thế nào để đảo ngược hàm số một chiều được nêu tóm tắt trong Phụ lục J. Tuy nhiên, có một câu hỏi cần được nói ngay ở đây. Nếu ai cũng biết N, tức chìa khóa mã công khai, thì biết đâu người ta cũng có thể suy ra p và q, chìa khóa riêng, và đọc được thư của Alice? Xét cho cùng, chính N được tạo bởi p và q. Tuy nhiên, thực tế, nếu N đủ lớn thì gần như không thể suy ra p và q từ N, và có lẽ đây chính là khía cạnh đẹp và tao nhã nhất của mật mã bất đối xứng RSA.

Alice đã tạo ra N bằng cách chọn p và q, rồi nhân chúng với nhau. Điểm cơ bản là ở chỗ, đó cũng chính là một hàm một chiều. Để minh họa bản chất một chiều của việc nhân các số nguyên tố, chúng ta có thể lấy hai số nguyên tố, ví dụ như 9.419 và 1.933, và nhân chúng với nhau. Với một máy tính cầm tay, sẽ chỉ mất vài giây là có ngay kết quả, 18.206.927. Tuy nhiên, nếu thay vì làm thế, người ta cho trước chúng ta số 18.206.927 và yêu cầu tìm các thừa số nguyên tố (hai số mà tích của chúng bằng 18.206.927) thì công việc sẽ mất thời gian hơn rất nhiều. Nếu bạn còn chưa tin vào mức độ khó khăn của việc tìm các thừa số nguyên tố, thì hãy thử làm ví dụ sau. Tôi chỉ mất 10 giây để tìm ra số 1.709.023, nhưng bạn và cái máy tính cầm tay chắc sẽ phải mất gần một buổi chiều mới có thể tính ra các thừa số nguyên tố.

Hệ thống mật mã bất đối xứng này, tức RSA, được gọi là dạng *mật mã chìa khóa công khai*. Để biết độ an toàn của RSA như thế nào, chúng ta có thể kiểm tra từ giác độ của Eve, và thử giải mã một bức thư của Alice gửi Bob. Để mã hóa thư gửi Bob, Alice

phải tìm chìa khóa công khai của Bob. Để tạo ra chìa khóa công khai của mình, Bob chọn các số nguyên tố là *pB* và *qB*, rồi nhân chúng với nhau tạo thành số *NB*. Bob giữ bí mật các số *pB* và *qB,* vì chúng chính là chìa khóa riêng của anh, nhưng anh cho công bố công khai *NB*, chẳng hạn là số 408.508.091. Alice nạp chìa khóa công khai của Bob là *NB* vào hàm mã hóa một chiều chung, và sau đó mã hóa thư gửi cho Bob. Khi thư mã hóa này đến nơi, Bob có thể đảo ngược hàm và giải mã nó bằng cách dùng các giá trị *pB* và *qB*. Trong khi đó, Eve chỉ bắt được bức thư trên đường gửi đi. Hy vọng giải mã duy nhất của cô là đảo ngược được hàm một chiều, và điều này chỉ có thể nếu cô biết *pB* và *qB*. Bob giữ bí mật *pB* và *qB*, song Eve, cũng như mọi người khác, đều biết *NB* là 408.508.091. Eve cố gắng suy ra các giá trị của *pB* và *qB* bằng cách tính xem các số nguyên tố nào có tích bằng 408.508.091, một quá trình được gọi là *phân tích ra thừa số nguyên tố*.

Quá trình phân tích ra thừa số rất mất thời gian, song chính xác thì phải mất bao lâu Eve mới tìm ra các thừa số nguyên tố của 408.508.091? Có rất nhiều cách để phân tích *NB* ra thừa số. Tuy có thể cách này nhanh hơn cách khác, song cách nào thì cũng đều phải kiểm tra xem mỗi số nguyên tố có phải là ước số của *NB* hay không. Chẳng hạn, 3 là số nguyên tố, song nó không phải là thừa số của 408.508.091, vì 408.508.091 không chia hết cho 3. Vì vậy, Eve tiếp tục chuyển qua số nguyên tố khác. Tương tự như vậy, 5 không phải là thừa số nên Eve lại tiếp tục thử số khác và cứ như vậy. Cuối cùng Eve dừng lại ở số 18.313, là số nguyên tố thứ 2000, thực sự là thừa số của 408.508.091. Sau khi tìm được một thừa số rồi thì dễ dàng tìm ra thừa số còn lại là 22.307. Nếu Eve có một máy tính và có thể kiểm tra bốn số nguyên tố trong

một phút thì sẽ phải mất 500 phút, hay hơn 8 giờ để tìm ra pB và qB. Nói cách khác, Eve có thể tính ra chìa khóa riêng của Bob trong vòng chưa đến một ngày và vì vậy có thể giải mã thư trong vòng chưa đến một ngày.

Đây chưa phải là độ an toàn rất cao, song Bob có thể lựa chọn số nguyên tố lớn hơn và bằng cách đó tăng độ an toàn của chìa khóa riêng. Chẳng hạn, anh có thể chọn số nguyên tố lớn cỡ 10^{65} (tức là số 1 và 65 số 0 tiếp sau, hay một trăm ngàn, triệu, triệu). Điều này sẽ tạo ra giá trị của N cỡ $10^{65} \times 10^{65} = 10^{130}$. Một máy tính có thể nhân hai số nguyên tố và cho N chỉ trong một giây, nhưng nếu Eve muốn đảo ngược quá trình để tìm p và q thì sẽ lâu hơn rất nhiều. Chính xác lâu bao nhiêu thì còn phụ thuộc vào tốc độ máy tính của Eve. Chuyên gia an ninh Simson Garfinkel đã ước tính rằng một máy tính Intel Pentium 100 MHz với RAM lớn cỡ 8MB sẽ phải mất 50 năm để phân tích ra thừa số nguyên tố một số lớn cỡ 10^{130}. Các nhà tạo mã hay có tính hoang tưởng và luôn xem xét đến tình huống xấu nhất, chẳng hạn như một âm mưu toàn thế giới muốn phá vỡ mật mã của họ. Vì vậy, Garfinkel quan tâm đến điều gì sẽ xảy ra nếu một trăm triệu máy tính cá nhân (số lượng máy tính đã bán ra năm 1995) liên kết lại với nhau. Kết quả là một số lớn cỡ 10^{130} có thể được phân tích ra thừa số nguyên tố chỉ trong vòng 15 giây. Do vậy, giờ đây độ an toàn thực sự được đông đảo chấp nhận là cần phải sử dụng các số nguyên tố thậm chí còn lớn hơn nữa. Đối với các giao dịch ngân hàng quan trọng, N thường tối thiểu có giá trị cỡ 10^{308}, tức lớn hơn 10 triệu tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ tỉ lần so với 10^{130}. Với nỗ lực của một trăm triệu máy tính cá nhân sẽ phải mất hơn 1000 năm mới phá vỡ được một

mật mã như vậy. Với giá trị đủ lớn của p và q, RSA quả là không gì thâm nhập nổi.

Lời cảnh báo duy nhất đối với độ an toàn của mật mã chìa khóa công khai RSA, đó là vào một lúc nào đó trong tương lai có ai đó tìm ra một cách phân tích ra thừa số của N nhanh hơn. Cũng có thể là một thập kỷ nữa hay thậm chí ngay ngày mai, một ai đó sẽ tìm ra một cách phân tích ra thừa số nhanh hơn và khi đó RSA sẽ trở nên vô dụng. Tuy nhiên, trong hơn 2000 năm qua, các nhà toán học đã rất cố gắng nhưng không thể tìm ra một cách tính tắt nào và ngay lúc này, việc phân tích ra thừa số nguyên tố vẫn còn là một tính toán tốn thời gian ghê gớm. Hầu hết các nhà toán học đều tin rằng việc phân tích ra thừa số nguyên tố bản thân nó vốn đã là một nhiệm vụ khó khăn và dường như có một quy tắc toán học nào đó ngăn cấm bất kỳ một tính toán tắt nào. Nếu chúng ta giả sử rằng họ đúng thì RSA dường như vẫn an toàn trong một tương lai gần.

Lợi thế to lớn của mật mã chìa khóa công khai RSA, đó là nó loại bỏ được tất cả những vấn đề của mật mã truyền thống, trong đó có vấn đề trao đổi chìa khóa mã. Alice không còn phải lo lắng về chuyện chuyển chìa khóa mã cho Bob một cách an toàn, hay Eve có thể bắt được chìa khóa mã. Thực tế, Alice không quan tâm có ai nhìn thấy chìa khóa công khai - càng nhiều người biết càng vui, vì chìa khóa công khai chỉ giúp cho việc mã hóa chứ không giúp gì cho việc giải mã. Chỉ còn một điều cần phải giữ bí mật đó chính là chìa khóa riêng để giải mã, và Alice có thể luôn giữ nó bên mình.

RSA được công bố lần đầu tiên vào tháng Tám năm 1977, khi Martin Gardner viết một bài báo có tựa đề "*Một loại mật mã mới*

mà phải mất hàng triệu năm nữa mới phá vỡ nổi" trong cột "Trò chơi Toán học" do ông phụ trách trên tờ *Scientific American*. Sau khi giải thích mật mã chìa khóa công khai hoạt động như thế nào, Gardner đã đưa ra một thách thức cho bạn đọc. Ông đã cho in một bản mật mã và cũng cung cấp luôn chìa khóa công khai được sử dụng để mã hóa nó:

N = 114.381.625.757.888.867.669.235.779.976.146.612.010.218.296.721.
242.362.562.561.842.935.706.935.245.733.897.830.597.123.563.
958.705.058.989.075.147.599.290.026.879.543.541

Thách đố ở đây là phân tích số *N* thành các thừa số nguyên tố *p* và *q*, và sử dụng các số này để giải mã thư. Giá trị giải thưởng là 100 đôla. Gardner không có đủ chỗ để giải thích thực chất của RSA, và thay vào đó ông yêu cầu bạn đọc viết thư cho Phòng Thí nghiệm về Khoa học Máy tính của MIT để họ gửi bản ghi nhớ kỹ thuật đã được chuẩn bị sẵn. Rivest, Shamir và Adleman rất kinh ngạc khi nhận được ba nghìn yêu cầu. Tuy nhiên, họ không trả lời ngay vì họ vẫn lo lắng sự công bố công khai ý tưởng của họ sẽ làm mất đi cơ hội được lấy bằng phát minh sáng chế. Khi bằng phát minh cuối cùng cũng được giải quyết, bộ ba đã tổ chức một bữa tiệc mừng mà tại đó các giáo sư và sinh viên vừa thưởng thức bánh pizza và bia vừa phải cho các bản ghi nhớ về kỹ thuật vào phong bì để gửi cho các độc giả của tờ *Scientific American*.

Đối với thách thức của Gardner, phải mất 17 năm mật mã đó mới được phá vỡ. Ngày 26 tháng Tư năm 1994, một nhóm gồm 600 người tình nguyện đã công bố các thừa số nguyên tố của *N* là:

q = 3.490.529.510.847.650.949.147.849.619.903.898.133.417. 764.638.493.387.843.990. 820.577

p = 32.769.132.993.266.709.549.961.988.190.834.461.413.177. 642.967.992.942.539.798.288.533

Sử dụng các giá trị này làm chìa khóa mã riêng, họ có thể giải mã được thư. Thư là một chuỗi các con số, song khi chuyển chúng thành các chữ cái thì được đọc là "các từ thần diệu là chim ưng biển khó tính". Việc phân tích ra thừa số được phân cho những người tình nguyện đến từ nhiều quốc gia khác nhau như Australia, Anh, Mỹ và Venezuela. Họ đã dành thời gian rảnh rỗi sử dụng các phòng máy tính, với các máy tính lớn và các siêu máy tính, mỗi người trong số họ phụ trách một phần công việc. Thực tế là, một hệ thống máy tính trên khắp thế giới đã hợp nhất và làm việc đồng thời để đối phó với thách thức của Gardner. Ngay cả khi luôn biết rằng có thể có những nỗ lực đồng thời cực lớn thì một số người đọc vẫn ngạc nhiên khi RSA lại bị phá vỡ trong một thời gian ngắn đến như vậy, song hãy nhớ rằng thách thức của Gardner đã sử dụng một giá trị tương đối nhỏ của N - mới chỉ cỡ 10^{129}. Ngày nay, những người sử dụng RSA thường chọn giá trị của N lớn hơn nhiều để đảm bảo an toàn cho những thông tin quan trọng. Giờ thì việc mã hóa thư bằng một giá trị N đủ lớn là việc bình thường nên tất cả các máy tính trên hành tinh sẽ phải cần thời gian lớn hơn tuổi của vũ trụ mới có thể hóa giải được mật mã đó.

Câu chuyện khác về Mật mã chìa khóa công khai

Trong hơn 20 năm qua, Diffie, Hellman và Merkle đã trở nên nổi tiếng thế giới vì đã phát minh ra khái niệm mật mã chìa khóa công khai, trong khi đó Rivest, Shamir và Adleman lại có công lao phát minh ra RSA, một sự thực thi đẹp nhất của mật mã chìa khóa công khai. Tuy nhiên, một tuyên bố mới đây cho thấy sách lịch sử sẽ phải được viết lại. Theo Chính phủ Anh, mật mã chìa khóa công khai thực sự đã được phát minh đầu tiên ở Tổng hành dinh Thông tin Liên lạc của Chính phủ (GCHQ) ở Cheltenham, một cơ quan tối mật được hình thành từ bộ phận còn lại của Bletchley Park sau Thế chiến Thứ hai. Đây là câu chuyện về tài khéo léo tuyệt vời, về những anh hùng vô danh và một sự che đậy của chính phủ đã kéo dài hàng thập kỷ.

Câu chuyện bắt đầu vào cuối những năm 1960, khi quân đội Anh bắt đầu lo ngại về vấn đề phân phối chìa khóa mã. Nhìn xa đến những năm 1970, các quan chức quân đội cấp cao đã hình dung ra một kịch bản, trong đó sự tiểu hình hóa các máy móc vô tuyến và sự giảm giá thành có nghĩa là mỗi người lính đều có thể liên tục liên lạc bằng vô tuyến với cấp trên của họ. Lợi thế của thông tin liên lạc trên diện rộng là rất lớn, song thông tin phải được mã hóa, mà vấn đề phân phối chìa khóa mã thì vẫn chưa khắc phục được. Đây là thời đại chỉ có dạng mã hóa đối xứng, nên chìa khóa mã phải được chuyển an toàn đến mỗi thành viên trong hệ thống liên lạc. Bất kỳ sự mở rộng liên lạc nào cuối cùng cũng sẽ bị chặn lại bởi gánh nặng của việc phân phối chìa khóa mã. Vào đầu năm 1969, quân đội đã yêu cầu James Ellis, một trong những nhà tạo mã hàng đầu của chính phủ Anh, tìm ra cách thức để đối phó với vấn đề phân phối chìa khóa mã.

Ellis là một nhân vật kỳ cục và hơi lập dị. Ông đã khoe một cách đầy tự hào rằng mình đã đi nửa vòng Trái đất thậm chí trước cả khi ông sinh ra - mẹ ông thụ thai ở Anh nhưng lại sinh ra ông ở Australia. Sau đó, khi vẫn còn là một đứa trẻ, ông trở về London và lớn lên ở khu Đông của thành phố này vào những năm 1920. Ở trường, sở thích chủ yếu của ông là khoa học, và ông theo học về vật lý ở trường Imperial College trước khi gia nhập Trạm Nghiên cứu Bưu điện ở Dollis Hill, nơi mà Tommy Flowers đã chế tạo ra máy Colossus, máy tính giải mã đầu tiên. Sau đó, Phòng mật mã ở Dollis Hill cuối cùng đã bị sáp nhập vào GCHQ, và vậy là ngày 1 tháng Tư năm 1965, Ellis chuyển đến Cheltenham là thành viên của một bộ phận mới hình thành là Nhóm An ninh Thông tin - Điện tử (CESG), một bộ phận đặc biệt của GCHQ nhằm mục đích đảm bảo an ninh cho thông tin liên lạc của nước Anh. Vì tham gia vào lĩnh vực an ninh quốc gia nên Ellis đã phải thề giữ bí mật nghề nghiệp của mình. Mặc dù vợ ông và gia đình đều biết rằng ông làm việc cho GCHQ song họ không hề biết gì về những khám phá của ông và không mảy may biết rằng ông là một trong những nhà tạo mã lỗi lạc nhất của quốc gia.

James Ellis

Mặc dù chuyên môn của ông là tạo mã, song Ellis chưa bao giờ được giao phụ trách bất kỳ nhóm nghiên cứu quan trọng nào của GCHQ. Ông rất lỗi lạc, song tính tình ông cũng rất thất thường, hướng nội và về bản chất ông không phải là người hợp với cách làm việc theo nhóm. Đồng nghiệp Richard Walton của ông nhớ lại:

> Ông là một nhân viên rất lắm mưu mẹo, và ông không thực sự thích hợp với công việc hằng ngày của GCHQ. Song về mặt bắt kịp các ý tưởng mới thì ông lại thật đặc biệt. Đôi khi bạn phải phân loại những thứ rác rưởi nhưng ông thì lại rất thích đổi mới và luôn muốn thách thức những gì có tính chất chính thống. Chúng tôi sẽ gặp rắc rối nếu ai ở GCHQ cũng giống như ông, song chúng tôi có thể dung nạp được một tỷ lệ cao những người như vậy hơn hầu hết các tổ chức khác. Chúng tôi chịu đựng được nhiều người như ông ấy.

Một trong những phẩm chất vĩ đại nhất của Ellis đó là kiến thức rộng lớn của ông. Ông đọc bất kỳ một tạp chí khoa học nào có trong tay, và không quẳng bất cứ thứ gì đi bao giờ. Vì lý do an ninh, các nhân viên của GCHQ phải dọn sạch bàn làm việc mỗi tối và cất mọi thứ vào các ngăn tủ có khóa, điều đó có nghĩa là các ngăn tủ của Ellis chất đầy những ấn phẩm vô danh nhất có thể tưởng tượng được. Ông nổi tiếng là một quân sư về mật mã, và nếu các nhà nghiên cứu khác có vấn đề nan giải nào, họ đều đến gõ cửa phòng ông với hy vọng kiến thức rộng lớn và tính độc đáo của ông sẽ giúp họ một giải pháp. Có lẽ vì danh tiếng này mà ông đã được yêu cầu giải quyết vấn đề phân phối chìa khóa mã.

Chi phí cho việc phân phối chìa khóa mã thực sự là rất lớn và sẽ trở thành nhân tố hạn chế sự mở rộng của mã hóa. Ngay cả khi chi phí phân phối chìa khóa mã đã giảm 10% thì cũng vẫn chiếm đáng kể ngân sách cho an ninh quân đội. Tuy nhiên, thay vì chỉ đơn giản ngồi gặm nhấm vấn đề, Ellis ngay lập tức bắt tay tìm kiếm một giải pháp triệt để và hoàn chỉnh. "Ông luôn tiếp cận vấn đề bằng cách hỏi 'Đây có phải thực sự là điều chúng ta muốn làm không?'", Walton kể, "James luôn là James, một trong những điều trước tiên ông làm đó là nghi ngờ yêu cầu cần phải chia sẻ thông tin bí mật, ở đây tôi muốn nói đó là chìa khóa mã. Không có định lý nào nói rằng bạn phải có một bí mật cần chia sẻ. Đây là điều không thể chấp nhận được".

Ellis bắt đầu tấn công vào vấn đề bằng cách tìm kiếm qua kho báu những bài báo khoa học của mình. Nhiều năm sau, ông đã ghi lại giây phút khi ông khám phá ra rằng phân phối chìa khóa mã không phải là một bộ phận tất yếu của mật mã.

> Sự kiện đã làm thay đổi quan điểm này chính là sự phát hiện ra một báo cáo của hãng Bell Telephone trong thời gian chiến tranh, không rõ tác giả, trong đó mô tả một ý tưởng tài tình về việc đảm bảo an toàn cho các cuộc nói chuyện điện thoại. Nó đề xuất rằng người nhận sẽ ngụy trang tiếng nói của người gửi bằng cách thêm tiếng ồn nhiễu vào đường dây. Sau đó anh ta sẽ khử nhiễu này đi, vì anh ta là người thêm nó vào nên phải biết rõ nó là thế nào. Bất lợi rõ ràng của hệ thống này về tính khả thi đã khiến nó không được sử dụng trong thực tế, song nó lại có một số những đặc điểm lý thú. Sự khác nhau giữa ý tưởng này và sự mã hóa thông thường là ở chỗ trong trường hợp này người nhận cũng tham gia vào quá trình mã hóa... Vậy là ý tưởng đã nảy sinh.

Tiếng ồn nhiễu là thuật ngữ chỉ bất kỳ một tín hiệu nào ảnh hưởng đến sự truyền thông tin. Thông thường nó được tạo bởi hiện tượng tự nhiên, và tính chất khó chịu nhất của nó là sự ngẫu nhiên hoàn toàn, tức là việc tách lọc tiếng ồn ra khỏi thông tin được truyền đi là rất khó khăn. Nếu một hệ thống vô tuyến được thiết kế tốt thì mức độ tiếng ồn thấp và thông tin nghe được rõ ràng, nhưng nếu mức độ tiếng ồn cao và át cả thông tin thì không có cách gì khôi phục lại được. Ellis đề xuất rằng người nhận, tức Alice, cố ý tạo nên tiếng ồn, mà cô có thể đo lường được trước khi thêm nó vào kênh liên lạc giữa cô và Bob. Sau đó Bob gửi một thông tin cho Alice và nếu Eve có ghi âm được kênh liên lạc, cô ta cũng sẽ không thể đọc được thông tin vì nó đã bị nhiễu bởi tiếng ồn. Eve không thể tách tiếng ồn đó ra khỏi thông tin. Người duy nhất có thể khử tiếng ồn và đọc được thông tin chính là Alice, vì chỉ có cô mới biết bản chất chính xác của tiếng ồn, sau khi đã bổ sung thêm nó vào lúc đầu. Ellis nhận thấy rằng, như vậy có thể đạt được độ an toàn mà không cần phải trao đổi bất kỳ chìa khóa mã nào. Chìa khóa mã chính là tiếng ồn, và chỉ Alice mới cần biết chi tiết của tiếng ồn đó.

Trong một bản ghi nhớ, Ellis đã mô tả chi tiết quá trình suy nghĩ của mình như sau: "Câu hỏi tiếp theo là hiển nhiên. Liệu điều này có thể làm được với cách mã hóa thông thường hay không? Liệu có thể tạo ra một bức thư mã hóa an toàn, người nhận có thể đọc được mà không cần phải trao đổi chìa khóa mã hay không? Câu hỏi này thực sự nảy ra một đêm, khi tôi đang nằm trên giường, và việc chứng minh tính khả thi về mặt lý thuyết chỉ mất có vài phút. Nghĩa là ở đây chúng ta đã có định lý tồn tại. Điều không thể nghĩ đến hóa ra lại thực sự có thể". (Một định

lý tồn tại chứng tỏ rằng một khái niệm cụ thể là có thể, nhưng không liên quan đến chi tiết của khái niệm đó). Nói cách khác, cho đến lúc này, việc tìm ra lời giải cho bài toán phân phối chìa khóa mã cũng giống như tìm một cái kim trong đống rơm, với khả năng là cái kim có thể không ở trong đó. Tuy nhiên, nhờ có định lý tồn tại, Ellis giờ đã biết rằng cái kim phải ở đâu đó trong đống rơm.

Ý tưởng của Ellis cũng tương tự như của Diffie, Hellman và Merkle, nhưng ông đã đi trước họ một vài năm. Tuy nhiên, không ai biết về thành quả của Ellis vì ông là nhân viên của Chính phủ Anh và vì vậy đã phải thề giữ bí mật. Cho đến cuối năm 1969, Ellis dường như đã rơi vào ngõ cụt như bộ ba ở Stanford năm 1975. Chính ông cũng đã chứng minh rằng mật mã chìa khóa công khai (hay mã hóa không bí mật như ông gọi) là có thể thực hiện được, và ông đã phát triển khái niệm chìa khóa công khai tách biệt với chìa khóa riêng. Ông cũng đã biết rằng ông phải tìm một hàm một chiều đặc biệt, có thể đảo ngược được nếu người nhận có một chút thông tin đặc biệt. Tiếc thay, Ellis không phải là một nhà toán học. Ông đã thử nghiệm với một vài hàm số toán học song ông nhanh chóng nhận ra rằng ông không thể tiến triển thêm nếu chỉ có một mình.

Đến lúc này, Ellis bèn báo cáo phát hiện của mình với cấp trên. Phản ứng của họ vẫn còn là tài liệu mật, song trong một cuộc phỏng vấn, Richard Walton đã chuẩn bị để diễn giải khá dài dòng với tôi về những bản ghi nhớ khác nhau đã được trao đổi. Ông ngồi xuống với chiếc valy nhỏ đặt trong lòng, nắp của nó che khuất các giấy tờ khỏi tầm nhìn của tôi, ông gõ nhẹ vào xấp tài liệu:

> Tôi không thể đưa ông xem các tài liệu mà tôi có ở đây vì vẫn còn những từ nhảm nhí như tối mật đóng dấu trên đó. Về cơ bản thì ý tưởng của James đã lên tới người ở cấp cao nhất, và nó đã được trưng dụng theo cách mà những người ở cấp cao nhất vẫn làm, để cho các chuyên gia có thể xem được. Họ tuyên bố là những gì James nói là tuyệt đối đúng. Nói cách khác, họ không thể gạch tên người đàn ông này như một kẻ lập dị. Đồng thời, họ không thể nghĩ ra cách nào để thực thi ý tưởng của ông trong thực tế. Và vì vậy họ rất ấn tượng trước tài năng của James song không chắc có cách nào tận dụng được lợi thế của nó.

Trong vòng ba năm sau, những bộ não thông minh nhất của GCHQ đã nỗ lực để tìm ra một hàm số một chiều thỏa mãn các yêu cầu của Ellis, song đã không thu được kết quả. Sau đó, vào tháng Chín năm 1973, thêm một nhà toán học gia nhập nhóm nghiên cứu. Clifford Cocks vừa mới tốt nghiệp Đại học Cambridge với chuyên ngành lý thuyết số, một trong những lĩnh vực toán học thuần túy nhất. Khi gia nhập GCHQ, ông mới biết rất ít về mã hóa cũng như thế giới bóng tối của thông tin liên lạc quân sự và ngoại giao, vì vậy người ta đã phân cho ông một cố vấn là Nick Patterson để hướng dẫn ông trong vài tuần đầu tiên ở GCHQ.

Sau khoảng sáu tuần, Patterson đã nói với Cocks về "một ý tưởng thực sự khác thường". Ông đã tóm tắt lý thuyết về mật mã chìa khóa công khai của Ellis và giải thích rằng hiện vẫn chưa có ai tìm ra một hàm số toán học thỏa mãn yêu cầu. Patterson kể với Cocks vì đó là ý tưởng "hot" nhất về mật mã lúc bấy giờ chứ không phải ông muốn Cocks thử giải quyết vấn đề đó. Tuy nhiên, như Cocks giải thích sau này, ông quyết định hành động:

“Không có gì đặc biệt xảy ra lúc đó, và vì vậy tôi nghĩ mình sẽ nghiền ngẫm về ý tưởng này. Vì tôi đã làm việc về lý thuyết số nên việc nghĩ về một hàm số một chiều, một thứ gì đó bạn có thể làm mà không làm ngược lại được, cũng là tự nhiên thôi. Các số nguyên tố và sự phân tích ra thừa số là một ứng viên tự nhiên và nó trở thành điểm khởi đầu của tôi”. Cocks bắt đầu tạo nên cái mà sau này được gọi là mật mã bất đối xứng RSA. Rivest, Shamir và Adleman tìm ra công thức về mật mã chìa khóa công khai của họ vào năm 1977, song bốn năm trước đó, chàng sinh viên trẻ tuổi vừa tốt nghiệp Đại học Cambridge cũng đã trải qua quá trình tư duy chính xác như vậy. Cocks nhớ lại: “Từ khi bắt đầu cho đến lúc kết thúc, tôi chỉ mất không quá nửa giờ đồng hồ. Tôi hoàn toàn hài lòng với bản thân mình. Tôi đã nghĩ, ‘ồ, thật tuyệt. Mình đã được giao một bài toán và mình đã giải được nó’”.

Cocks không đánh giá được đầy đủ tầm quan trọng của khám phá của ông. Ông hoàn toàn không biết rằng thực tế là những bộ não ưu tú nhất của GCHQ đã vật lộn với vấn đề này trong suốt ba năm, và ông cũng không hề có ý niệm gì về chuyện mình đã làm nên một trong những đột phá quan trọng nhất thế kỷ về khoa học mật mã. Sự ngây thơ của Cocks có thể là một phần lý do cho sự thành công của ông, cho phép ông giải quyết vấn đề với sự tự tin chứ không phải chạm vào nó một cách rụt rè. Cocks nói với người cố vấn về khám phá của mình và chính là Patterson sau đó đã báo cáo cho ban giám đốc. Cocks vốn khá nhút nhát và vẫn còn là một tân binh trong khi Patterson đánh giá được đầy đủ bối cảnh của vấn đề và có khả năng hơn trong việc xử lý những vấn đề kỹ thuật không tránh khỏi nảy sinh.

Clifford Cocks

Ngay lập tức, nhiều người hoàn toàn xa lạ bắt đầu vây lấy Cocks, cậu bé thần đồng, và bắt đầu chúc mừng ông. Một trong những người xa lạ này là James Ellis, ông rất muốn gặp người đã biến giấc mơ của ông thành hiện thực. Vì Cocks vẫn còn chưa hiểu được tầm cỡ thành công của mình nên chi tiết của cuộc gặp mặt này không để lại một ấn tượng lớn nào và vì vậy giờ đây, hơn hai thập kỷ sau, ông không còn nhớ gì về phản ứng của Ellis.

Khi Cocks cuối cùng cũng ý thức được việc mình đã làm, ông hiểu rằng khám phá của ông có thể làm thất vọng G. H. Hardy, một trong những nhà toán học lỗi lạc nhất nước Anh của nửa đầu thế kỷ. Trong cuốn *Lời biện bạch của nhà toán học*, được viết vào năm 1940, Hardy đã tuyên bố rất tự hào rằng: "Toán học thực sự không có ảnh hưởng gì đến chiến tranh. Càng chưa có ai khám phá ra lý thuyết số đã phục vụ gì cho mục đích chiến tranh." Nhưng toán học thực sự, tức là toán học thuần túy, chẳng hạn như lý thuyết số, lại là cốt lõi của thành quả của Cocks. Cocks đã chứng minh rằng Hardy đã sai. Tính phức tạp của lý thuyết số giờ đây đã được sử dụng để giúp cho các tướng lĩnh lập kế hoạch các trận đánh của họ một cách bí mật hoàn toàn. Vì thành công của ông được ứng dụng cho thông tin liên lạc của quân đội

nên Cocks, cũng giống như Ellis, đã bị cấm không được nói với ai bên ngoài GCHQ về những việc họ đã làm. Làm việc tại một tổ chức chính phủ tối mật có nghĩa là ông không thể nói với bố mẹ mình lẫn các đồng nghiệp cũ ở Đại học Cambridge. Chỉ một người duy nhất ông có thể nói, đó chính là Gill, vợ ông, vì bà cũng là một nhân viên của GCHQ.

Mặc dù ý tưởng của Cocks là một trong những bí mật lớn nhất của GCHQ song nó lại khổ vì đã đi trước thời đại. Cocks đã khám phá ra một hàm số toán học cho phép sử dụng được mật mã chìa khóa công khai, song việc thực hiện hệ thống vẫn còn rất khó khăn. Mã hóa bằng mật mã chìa khóa công khai đòi hỏi máy tính phải mạnh hơn nhiều so với mã hóa bằng mật mã đối xứng như DES. Vào đầu những năm 1970, máy tính vẫn còn tương đối thô sơ và không thể thực hiện được quá trình mã hóa với chìa khóa công khai trong một khoảng thời gian hợp lý. Vì vậy, GCHQ rơi vào tình thế không thể khai thác được mật mã này. Cocks và Ellis đã chứng minh được điều rõ ràng không thể là có thể, song không ai tìm ra cách nào để thực hiện được nó trong thực tế.

Đầu năm sau, năm 1974, Cocks đã giải thích về mật mã chìa khóa công khai với Malcolm Williamson, người mới được tuyển vào GCHQ. Họ tình cờ lại là bạn cũ của nhau. Cả hai đều đã học ở trường Manchester Grammar School, nơi mà phương châm của trường là *Sapere aud,* có nghĩa là "Dám là thông thái". Khi học ở trường này vào năm 1968, hai cậu bé đã đại diện cho nước Anh cùng đi dự cuộc thi Olympic toán quốc tế ở Liên Xô. Sau khi cùng học ở trường Đại học Cambridge, họ đã theo đuổi những con đường khác nhau trong hai năm, nhưng giờ đây họ gặp lại

Malcolm Williamson

nhau ở GCHQ. Họ đã trao đổi các ý tưởng về toán học từ lúc 11 tuổi, song khám phá của Cocks về mật mã chìa khóa công khai là một ý tưởng gây sốc nhất mà Williamson đã từng được nghe. "Cliff giải thích ý tưởng của cậu ấy với tôi," Williamson nhớ lại, "và tôi thực sự không thể tin được. Tôi rất ngờ vực, vì đó là điều rất kỳ dị để có thể thực hiện được".

Williamson bỏ đi và bắt đầu tìm cách chứng minh rằng Cocks đã phạm một sai lầm nào đó và rằng mật mã chìa khóa công khai là thực sự không tồn tại. Ông kiểm tra về mặt toán học, với mong muốn tìm ra một sai sót ẩn giấu trong đó. Mật mã chìa khóa công khai dường như quá tuyệt vời để trở thành sự thật và Williamson quyết định phải tìm cho ra sai lầm, nên ông mang công việc về nhà. Nhân viên của GCHQ không được phép mang công việc về nhà vì tất cả mọi thứ họ làm đều là bí mật và môi trường ở nhà có thể dễ bị gián điệp rình mò. Tuy nhiên, vấn đề này cứ ám ảnh trong đầu Williamson nên ông không thể tránh suy nghĩ về nó. Bất chấp luật lệ, ông đã mang việc về nhà làm. Ông đã cố tìm ra một sai sót nào đó trong suốt năm giờ liền. "Cuối cùng thì tôi thất bại," Williamson

kể, "Thay vào đó, tôi đã đi tới một giải pháp khác cho vấn đề phân phối chìa khóa mã". Williamson đã khám phá ra cách trao đổi chìa khóa mã Diffie-Hellman-Merkle, gần như đồng thời với Martin Hellman. Phản ứng ban đầu của Williamson phản ánh bản tính hay bi quan của ông: "Nó thật tuyệt, tôi tự nghĩ như vậy. Nhưng tôi vẫn băn khoăn tự hỏi liệu có một sai sót nào trong đó không. Tôi nghĩ hôm đó tâm trạng của tôi không được tốt".

Vào năm 1975, James Ellis, Clifford Cocks và Malcolm Williamson đã khám phá ra tất cả những khía cạnh cơ bản của mật mã chìa khóa công khai nhưng tất cả họ đều phải giữ im lặng. Bộ ba người Anh đã phải ngồi lại phía sau để nhìn khám phá của mình được khám phá lại bởi Diffie, Hellman, Merkle, Rivest, Shamir và Adleman trong hơn ba năm sau. Điều kỳ lạ là, khám phá về RSA của GCHQ lại ra đời trước trao đổi chìa khóa mã Diffie-Hellman-Merkle, trong khi ở thế giới bên ngoài, trao đổi chìa khóa mã Diffie-Hellman-Merkle lại ra đời trước. Báo chí khoa học đưa tin về những khám phá tại Stanford và MIT, và các nhà nghiên cứu, những người được phép công bố công khai thành quả của họ trên các tạp chí khoa học trở nên nổi tiếng trong cộng đồng các nhà tạo mã. Chỉ cần xem qua bằng công cụ tìm kiếm trên Internet sẽ thấy 15 trang Web đề cập đến Clifford Cocks, so với 1.382 trang nhắc đến Whitfield Diffie. Thái độ kiềm chế của Cocks thật đáng khâm phục: "Không nên dây dưa vào chuyện này để được công chúng biết tới". Williamson cũng bình thản như vậy: "Phản ứng của tôi là 'Tốt thôi, lẽ đời là thế mà'. Điều quan trọng là tôi phải tiếp tục tiến tới trong phần đời còn lại của mình".

Hình 69. Malcolm Williamson (người thứ hai từ trái) và Clifford Cocks (người ngoài cùng bên phải) đến dự cuộc thi Olympic toán quốc tế năm 1968

Nỗi day dứt duy nhất của Williamson đó là GCHQ không lấy được bằng phát minh về mật mã chìa khóa công khai. Khi Cocks và Williamson lần đầu tiên làm nên khám phá của mình, có một sự thỏa thuận trong ban giám đốc GCHQ là việc cấp bằng phát minh là không thực hiện được vì hai lý do. Thứ nhất, việc cấp bằng sẽ có nghĩa là phải công bố chi tiết công việc của họ, điều này mâu thuẫn với mục đích của GCHQ. Thứ hai, vào đầu những năm 1970, việc các thuật toán toán học có được cấp bằng phát minh hay không còn chưa rõ ràng. Tuy nhiên, khi Diffie và Hellman thử nộp hồ sơ xin cấp bằng phát minh vào năm 1976, rõ ràng là họ đã được cấp. Lúc đó, Williamson đã muốn công khai và ngăn chặn việc đăng ký của Diffie và Hellman, song ông đã bị các nhà quản lý cao cấp chặn lại, họ không có tầm nhìn đủ xa để thấy trước được cuộc cách mạng kỹ thuật số và tiềm năng của mật mã chìa khóa công khai. Cho đến đầu những năm 1980, các vị lãnh đạo của Williamson mới bắt đầu hối tiếc về quyết định của

mình, vì sự phát triển của máy tính và thời kỳ đầu của Internet đã chứng tỏ rằng RSA và trao đổi chìa khóa mã Diffie-Hellma-Merkle đều là những sản phẩm thương mại cực kỳ thành công. Năm 1996, Công ty An toàn Dữ liệu RSA, chịu trách nhiệm về sản phẩm RSA, đã được bán với giá 200 triệu đôla.

Tuy công việc tại GCHQ vẫn còn là bí mật, song có một tổ chức khác đã biết tới những đột phá đã đạt được ở Anh. Vào đầu những năm 1980, Cơ quan An ninh Quốc gia Mỹ đã biết về công việc của Ellis, Cocks và Williamson, và cũng có thể thông qua NSA (Cơ quan an ninh quốc gia) mà Whitfield Diffie đã nghe được tin đồn về những khám phá ở Anh. Tháng Chín năm 1982, Diffie quyết định phải xem tin đồn đó có phải là sự thật hay không. ông cùng với vợ đã tới Cheltenham để nói chuyện mặt đối mặt với James Ellis. Họ gặp nhau trong một quán rượu địa phương và Mary rất nhanh chóng bị choáng trước tính cách khác thường của Ellis:

> Chúng tôi ngồi nói chuyện, và tôi chợt nhận ra rằng đây là một con người tuyệt vời nhất mà bạn có thể tượng tượng ra. Kiến thức rộng lớn của ông về toán học không phải là điều mà tôi có thể tự tin bình luận, song ông ấy thực sự là một chính nhân, cực kỳ khiêm tốn, một người với tâm hồn vô cùng hào phóng và quý phái. Tôi nói quý phái ở đây không có nghĩa là lạc hậu và cổ hủ. Người đàn ông đó là một hiệp sĩ. Ông ấy là một người đàn ông tốt, thực sự tốt. Ông ấy có một tâm hồn rất cao quý.

Diffie và Ellis đã thảo luận với nhau về nhiều chủ đề khác nhau, từ khảo cổ học cho đến những con chuột rơi vào thùng rượu làm cải thiện hương vị của rượu táo ra sao, nhưng cứ khi

nào câu chuyện hướng về mật mã thì Ellis lại khéo léo thay đổi đề tài. Cuối cuộc gặp, khi sắp phải chia tay, Diffie không đừng được nữa đã hỏi thẳng Ellis câu hỏi thường trực trong tâm trí ông: "Hãy cho tôi biết về việc ông đã phát minh ra mật mã chìa khóa công khai như thế nào?". Im lặng một lúc lâu, cuối cùng Ellis mới thì thào: "ồ, tôi không biết nên nói như thế nào. Tôi chỉ biết nói rằng các ông đã làm được điều đó nhiều hơn chúng tôi".

Mặc dù GCHQ đã khám phá ra mật mã chìa khóa công khai đầu tiên, song điều đó không hề làm giảm bớt thành công của các nhà khoa học đã khám phá lại nó. Chính các nhà khoa học này là những người đầu tiên nhận ra tiềm năng của mã hóa bằng chìa khóa công khai, và cũng chính họ đã làm cho nó trở nên thực hiện được. Hơn nữa, hoàn toàn có khả năng là GCHQ sẽ không bao giờ công bố thành công của họ, do đó sẽ ngăn chặn một dạng mã hóa có thể làm cho cuộc cách mạng kỹ thuật số đạt tới tiềm năng đầy đủ của nó. Cuối cùng, sự khám phá bởi các nhà khoa học này hoàn toàn độc lập với khám phá của GCHQ, và dựa trên những trí tuệ ngang tầm với nó. Môi trường khoa học hoàn toàn biệt lập với phạm vi tối mật của những nghiên cứu thuộc diện mật và các nhà khoa học không thể tiếp cận với các công cụ và tri thức bí mật được che giấu trong thế giới bí mật đó. Trái lại, các nhà nghiên cứu của chính phủ luôn tiếp cận được với các tài liệu khoa học bên ngoài. Người ta có thể nghĩ về luồng thông tin này như là một hàm số một chiều - thông tin chảy tự do theo một chiều, song nó bị cấm gửi theo chiều ngược lại.

Khi Diffie nói với Hellman về Ellis, Cocks và Williamson, thái độ của ông là những khám phá của các nhà khoa học sẽ được

coi là một chú thích trong lịch sử những nghiên cứu bí mật và khám phá của GCHQ cũng sẽ được coi là một chú thích trong lịch sử nghiên cứu khoa học. Tuy nhiên, ở giai đoạn này, không ai, ngoại trừ GCHQ, NSA, Diffie và Hellman, được biết về các nghiên cứu được xếp loại là bí mật, nên nó thậm chí còn chưa được coi như là một chú thích.

Cho đến giữa những năm 1980, thái độ của GCHQ thay đổi và ban giám đốc đã xem xét đến việc công bố rộng rãi các công trình của Ellis, Cocks và Williamson. Toán học của mật mã chìa khóa công khai đã thực sự được công bố trên phạm vi rộng rãi, và dường như không còn lý do gì để tiếp tục giữ bí mật nữa. Thực tế, sẽ có những lợi ích khác nếu như người Anh tiết lộ những công trình đột phá của họ về mật mã chìa khóa công khai. Như Richard Walton nhớ lại:

> Chúng tôi đã đùa cợt với ý tưởng về việc giải mật vào năm 1984. Chúng tôi bắt đầu nhìn ra lợi ích của việc GCHQ được biết đến rộng rãi hơn. Đó là thời điểm mà thị trường an ninh của chính phủ được mở rộng ra ngoài những khách hàng quân đội và ngoại giao truyền thống, và chúng tôi cần phải thu hút sự tin tưởng của những người chưa từng giao dịch với chúng tôi. Chúng tôi lúc đó đang ở giữa thời kỳ cầm quyền của Thatcher và chúng tôi đang cố gắng chống lại một thứ quan niệm "chính phủ thì xấu, tư nhân thì tốt". Vì vậy, chúng tôi đã có ý định công bố một bài báo, song ý tưởng này đã bị kẻ phá hoại là Peter Wright, tác giả của cuốn Spycatcher, làm hỏng mất. Chúng tôi chỉ công kích ban lãnh đạo cao cấp thông qua bài báo này khi tất cả đang loạn xạ cả lên về cuốn Spycatcher. Sau đó thì mệnh lệnh của ngày hôm đó là "cúi đầu xuống, đội mũ lên".

Peter Wright là một nhân viên tình báo Anh đã về hưu và việc xuất bản *Spycatcher*, cuốn hồi ký của ông, đã gây ra những bối rối lớn của chính phủ Anh. Vì vậy phải đến 13 năm sau GCHQ cuối cùng mới công bố công khai - tức 28 năm sau đột phá ban đầu của Ellis. Năm 1997, Clifford Cocks đã hoàn thành một công trình quan trọng không thuộc diện mật về RSA và nó chắc chắn sẽ được cộng đồng rộng rãi hơn quan tâm và sẽ không có rủi ro gì về an ninh nếu nó được công bố. Vì vậy, ông đã được đến mời trình bày tại Hội nghị của Viện Toán học và ứng dụng được tổ chức tại Cirencester. Căn phòng chắc sẽ có đông đảo các chuyên gia về mật mã. Một ít người trong số họ chắc biết rằng Cocks, người sẽ chỉ nói về một khía cạnh của RSA, thực sự là nhà phát minh không được thừa nhận. Có nguy cơ là rất có thể có ai đó sẽ đặt ra những câu hỏi dễ gây lúng túng, đại loại như "Ông đã phát minh ra RSA phải không?". Nếu có một câu hỏi như vậy, không biết Cocks sẽ trả lời thế nào? Theo chính sách của GCHQ, ông sẽ phải chối bỏ vai trò của mình trong việc phát minh ra RSA, và do đó ông buộc sẽ phải nói dối về một vấn đề gì đó hoàn toàn vô hại. Tình huống này rõ ràng sẽ rất kỳ cục và GCHQ quyết định đã đến lúc phải thay đổi chính sách của họ. Cocks được phép bắt đầu bài nói bằng việc giới thiệu tóm tắt câu chuyện về sự đóng góp của GCHQ với mật mã chìa khóa công khai.

Vào ngày 18 tháng Mười hai năm 1997, Cocks đã trình bày báo cáo của mình. Sau gần ba thập kỷ bí mật, Ellis, Cocks và Williamson đã nhận được sự thừa nhận mà họ xứng đáng được hưởng. Đáng buồn là James Ellis đã mất chỉ một tháng trước đó, vào ngày 25 tháng Mười một năm 1997, ở tuổi 73. Ellis đã gia nhập vào danh sách những chuyên gia mật mã Anh, mà đóng

góp của họ chưa bao giờ được thừa nhận lúc họ còn đang sống. Sự hóa giải mật mã Vigenère của Charles Babbage cũng không được tiết lộ khi ông còn sống vì thành quả của ông là vô giá đối với quân đội Anh ở Cộng hòa tự trị Crimea. Thay vì, công lao đó lại thuộc về Friedrich Kasiski. Tương tự như vậy, đóng góp của Alan Turing vào những nỗ lực trong chiến tranh là vô song, nhưng bí mật chính phủ đòi hỏi công việc của ông đối với Enigma không thể được tiết lộ.

Năm 1987, Ellis đã viết một tài liệu mật ghi lại đóng góp của ông đối với mật mã chìa khóa công khai, trong đó có cả những suy nghĩ của ông về việc giữ bí mật vẫn thường bao quanh công việc liên quan đến mật mã:

> Khoa học mật mã là một khoa học khác thường nhất. Hầu hết các nhà khoa học chuyên nghiệp đều muốn là người đầu tiên công bố thành quả của mình, bởi lẽ thông qua việc phổ biến thì công trình mới thể hiện được giá trị của nó. Trái lại, giá trị đầy đủ nhất của khoa học mật mã lại được xác định bởi việc hạn chế đến mức thấp nhất những thông tin sẵn có lọt vào tay kẻ thù tiềm tàng. Những nhà tạo mã chuyên nghiệp thường làm việc trong những cộng đồng khép kín để có sự tương tác chuyên nghiệp vừa đủ để đảm bảo chất lượng trong khi vẫn duy trì được bí mật đối với người ngoài. Việc tiết lộ những bí mật này thường chỉ được cho phép vì lợi ích của tính chính xác lịch sử sau khi đã được chứng minh là nó không còn thu được lợi ích gì thêm từ việc tiếp tục giữ bí mật nữa.

7

Riêng tư tốt đẹp

Đúng như Whit Diffie đã tiên đoán vào đầu những năm 1970, giờ đây chúng ta đang bước vào Kỷ nguyên Thông tin, thời kỳ hậu công nghiệp trong đó thông tin là loại hàng hóa có giá trị nhất. Sự trao đổi thông tin số hóa trở thành một phần không thể thiếu trong xã hội chúng ta. Giờ đây hàng chục triệu thư điện tử *(e-mail)* được gửi đi mỗi ngày và e-mail chẳng bao lâu nữa sẽ trở nên phổ biến hơn cả thư thông thường. Internet, dù vẫn còn đang trong thời kỳ non trẻ, đã cung cấp cơ sở hạ tầng cho thương trường số hóa và thương mại điện tử cũng đang phát triển mạnh. Tiền được lưu chuyển qua hệ thống mạng máy tính *(cyberspace)* và người ta ước đoán rằng mỗi ngày một nửa GDP của thế giới dịch chuyển qua khu vực hệ thống viễn thông tài chính liên ngân hàng toàn cầu. Trong tương lai, các xã hội dân chủ thích trưng cầu dân ý sẽ bắt đầu thực hiện việc bỏ phiếu trực tuyến trên mạng, và các chính phủ sẽ sử dụng Internet vào việc điều hành đất nước, mang lại những tiện ích như khai thuế trực tiếp trên mạng, chẳng hạn.

Tuy nhiên, thành công của Kỷ nguyên Thông tin lại phụ thuộc vào khả năng bảo vệ thông tin lưu chuyển khắp thế giới, và điều đó lại phụ thuộc vào sức mạnh của khoa học mật mã. Mã hóa hiện có thể được coi như là cung cấp khóa và chìa khóa cho Kỷ nguyên Thông tin. Trong hai ngàn năm, mã hóa là cực kỳ quan trọng chỉ đối với chính phủ và quân đội, song ngày nay nó cũng có một vai trò không nhỏ trong việc tạo những tiện ích cho các doanh nghiệp, và nay mai, những người bình thường cũng sẽ dựa vào khoa học mật mã để bảo vệ những bí mật riêng tư của mình. May mắn là vừa đúng lúc Kỷ nguyên Thông tin bùng nổ, thì chúng ta lại được tiếp cận với những mật mã cực mạnh. Sự phát minh ra mật mã chìa khóa công khai, đặc biệt là mật mã RSA, đã mang lại cho các nhà tạo mã ngày nay một lợi thế rõ rệt trong cuộc chiến khốc liệt và liên tục với các nhà giải mã. Nếu giá trị của N đủ lớn thì việc tìm ra p và q sẽ khiến Eve mất quá nhiều thời gian, và vì vậy mã hóa bằng RSA là thực sự không thể phá vỡ được. Điều quan trọng hơn cả, đó là mật mã chìa khóa công khai không bị làm cho yếu đi bởi bất kỳ vấn đề phân phối chìa khóa mã nào. Nói tóm lại, RSA bảo đảm cung cấp những cái khóa không thể phá được cho những thông tin quý giá nhất của chúng ta.

Tuy nhiên, cũng như mọi công nghệ khác, việc mã hóa vẫn còn có mặt tối của nó. Đồng thời với việc bảo vệ thông tin của những công dân tuân thủ pháp luật thì mã hóa cũng bảo vệ thông tin cho bọn tội phạm và những tên khủng bố. Hiện nay, cảnh sát sử dụng thủ đoạn nghe trộm như là một cách để thu thập bằng chứng về những trường hợp nghiêm trọng, như tội phạm có tổ chức và khủng bố, song điều này có thể sẽ không thực hiện được nếu bọn tội phạm sử dụng loại mật mã không thể phá nổi. Vì

chúng ta đang bước vào thế kỷ 21, tình trạng tiến thoái lưỡng nan chủ yếu của khoa học mật mã, đó là phải tìm ra một cách cho phép công chúng và các doanh nghiệp sử dụng việc mã hóa để tận dụng lợi thế của Kỷ nguyên Thông tin mà không cho phép bọn tội phạm lạm dụng việc mã hóa và trốn khỏi sự truy nã. Hiện đang có một cuộc tranh luận sôi động và gay gắt về con đường phát triển tối ưu và phần lớn cuộc thảo luận được khơi gợi từ câu chuyện về Phil Zimmermann, người đã nỗ lực thúc đẩy việc sử dụng mã hóa một cách rộng rãi, khiến cho các chuyên gia an ninh Mỹ hoảng sợ, đe dọa đến hiệu lực của Cơ quan An ninh Quốc gia, cơ quan ngốn hàng tỉ đôla và khiến ông trở thành đối tượng truy nã của FBI và của một cuộc điều tra xét xử lớn.

Phil Zimmermann học vật lý và sau đó là tin học vào giữa những năm 1970 tại Đại học Florida Atlantic. Sau khi tốt nghiệp, ông dự định sẽ kiếm một công việc ổn định trong lĩnh vực công nghiệp máy tính đang ngày càng lớn mạnh nhanh chóng, song những sự kiện chính trị vào đầu những năm 1980 đã làm thay đổi cuộc đời ông, và ông không còn quan tâm mấy đến công nghệ chíp silicon nữa mà lo lắng nhiều hơn đến sự đe dọa của chiến tranh hạt nhân. Ông lo ngại sự tấn công của Liên Xô vào Afganistan, cuộc bầu cử của Ronald Regan, sự bất ổn có

Phil Zimmermann

thể gây ra bởi một Brezhnev già nua và bản chất căng thẳng ngày càng tăng của cuộc chiến tranh lạnh. Ông thậm chí còn nghĩ đến việc chuyển cả gia đình đến New Zealand, vì tin rằng đó là một trong số ít nơi trên Trái đất này có thể trú ngụ được sau cuộc chiến tranh hạt nhân. Song ngay khi ông nhận được hộ chiếu và các giấy tờ nhập cư cần thiết, ông và vợ ông đã tham gia một cuộc họp do tổ chức Chiến dịch Đóng băng Vũ khí Hạt nhân tổ chức. Thay vì trốn chạy, gia đình Zimmermann đã quyết định ở lại và tham gia chiến đấu tại nhà, trở thành những người hoạt động chống hạt nhân hàng đầu - họ đã giáo dục cho những ứng cử viên chính trị về vấn đề chính sách quân sự, và bị bắt tại khu vực thử hạt nhân ở Nevada cùng với 400 người phản đối khác.

Vài năm sau, năm 1988, Mikhail Gorbachev trở thành người đứng đầu Liên bang Xô viết, báo hiệu thời kỳ cải tổ, công khai và giảm bớt căng thẳng Đông - Tây. Nỗi sợ hãi của Zimmermann bắt đầu lắng dịu, song niềm đam mê hoạt động chính trị của ông không hề suy giảm, chỉ có điều nó chuyển sang một hướng khác. Ông bắt đầu tập trung sự quan tâm của mình đến cuộc cách mạng số hóa và sự cần thiết phải mã hóa:

> Khoa học mật mã đã từng là một môn khoa học bí mật, có liên quan rất ít đến cuộc sống hằng ngày. Trong lịch sử, nó luôn có một vai trò đặc biệt trong thông tin liên lạc của quân đội và ngoại giao. Song trong Kỷ nguyên Thông tin, khoa học mật mã là sức mạnh chính trị, và đặc biệt là mối quan hệ quyền lực giữa một chính phủ và nhân dân của nó. Đó là quyền được riêng tư, quyền tự do ngôn luận, tự do liên kết chính trị, tự do báo chí, tự do không bị điều tra và bắt bớ vô lý, tự do được yên thân.

Những quan điểm này dường như là hoang tưởng, song theo Zimmermann, có sự khác nhau căn bản giữa thông tin liên lạc truyền thống và truyền thông số hóa, và sự khác biệt này có những hậu quả quan trọng đối với an ninh:

> Trong quá khứ, nếu chính phủ muốn xâm phạm đến bí mật riêng tư của những công dân bình thường, thì nó phải tốn công để chặn bắt, hơ hơi nước để bóc và đọc thư, hay nghe và chép lại những cuộc đối thoại trên điện thoại. Điều này cũng tương tự như việc bắt cá bằng lao và dây, mỗi lần chỉ bắt được một con. May mắn thay cho tự do và dân chủ, kiểu quản lý cần nhiều nhân công này là phi thực tế trên quy mô lớn. Ngày nay, thư điện tử đang dần thay thế cho thư viết trên giấy truyền thống và chẳng bao lâu nữa sẽ trở thành chuẩn mực cho mọi người, và giờ đây nó không phải là thứ gì mới mẻ nữa. Không giống như thư viết trên giấy, thư điện tử quá dễ chặn bắt và quét tìm những từ then chốt đáng chú ý. Việc này có thể thực hiện được dễ dàng, thường xuyên, tự động và không bị phát hiện trên quy mô lớn.

Sự khác nhau giữa thư thường và thư số hóa có thể được minh họa bằng cách tưởng tượng rằng Alice muốn gửi thư mời dự tiệc sinh nhật và Eve, người không được mời, muốn biết thời gian và địa điểm của bữa tiệc đó. Nếu Alice sử dụng cách gửi thư truyền thống qua bưu điện, thì Eve sẽ rất khó mà chặn bắt được một trong các giấy mời đó. Trước hết, Eve không biết các giấy mời của Alice đi vào hệ thống bưu điện từ đâu, vì Alice có thể sử dụng bất kỳ hòm thư bưu điện nào trong thành phố. Hy vọng duy nhất của cô ta bắt được một giấy mời là bằng cách nào

đó xác định được địa chỉ của một trong những người bạn của Alice, và đột nhập vào phòng phân loại của trạm bưu điện địa phương. Sau đó kiểm tra từng lá thư một. Nếu tìm được một lá thư từ Alice, Eve sẽ mở nó ra để biết thông tin mà mình muốn, rồi sau đó lại đặt trả lại như ban đầu để tránh mọi sự nghi ngờ là đã có sự bóc trộm.

Trong khi đó, nhiệm vụ của Eve sẽ đơn giản hơn nhiều, nếu Alice gửi giấy mời qua thư điện tử. Khi thư rời khỏi máy tính của Alice, chúng sẽ đến một máy chủ địa phương, một lối vào chính trên Internet; nếu Eve đủ thông minh, cô có thể xâm nhập vào máy chủ địa phương mà không phải ra khỏi nhà. Giấy mời sẽ có địa chỉ e-mail của Alice và sàng lọc ra các thư điện tử có chứa địa chỉ của Alice chỉ là một việc hết sức tầm thường. Một khi giấy mời được tìm thấy thì không phải mở phong bì và vì vậy không khó khăn gì đọc được nó. Hơn nữa, giấy mời có thể được gửi theo cách mà không có bất kỳ dấu hiệu nào chứng tỏ đã bị chặn bắt. Alice sẽ không biết điều gì đã xảy ra. Tuy nhiên, có một cách ngăn chặn Eve không đọc được thư điện tử của Alice, đó chính là mã hóa.

Hơn một trăm triệu thư điện tử được gửi khắp thế giới mỗi ngày và chúng đều rất dễ bị chặn bắt. Công nghệ kỹ thuật số đã hỗ trợ cho thông tin liên lạc song nó cũng làm nảy sinh khả năng các thông tin này dễ bị kiểm soát. Theo Zimmermann, các nhà tạo mã có nhiệm vụ phải khuyến khích việc sử dụng mã hóa và nhờ đó bảo vệ được những bí mật riêng tư của mỗi cá nhân:

> Một chính phủ trong tương lai có thể thừa hưởng một cơ sở hạ tầng công nghệ rất lạc quan cho việc giám sát, trong đó họ

có thể quan sát được những bước đi của đối thủ chính trị, mọi giao dịch tài chính, mọi thông tin liên lạc, mọi mẩu thư điện tử, mọi cuộc gọi điện thoại. Tất cả đều có thể bị xâm nhập, theo dõi và nhận biết một cách tự động nhờ công nghệ nhận biết giọng nói và bị ghi lại. Đây là lúc mà khoa học mật mã phải bước ra khỏi bóng tối của tình báo và quân đội, để bước ra ánh sáng và để cho những người còn lại chúng ta nắm lấy.

Về lý thuyết, khi RSA được phát minh vào năm 1977, nó như là một liều thuốc giải cho kịch bản độc tài đạo đức giả, bởi vì giờ đây các cá nhân cũng có thể tự tạo các chìa khóa mã công khai và chìa khóa mã riêng, sau đó gửi và nhận thư từ một cách tuyệt đối an toàn. Tuy nhiên, trong thực tế, vẫn còn một vấn đề lớn, đó là vì quá trình mã hóa RSA thực sự đòi hỏi phải có những máy tính mạnh hơn rất nhiều so với khi dùng các dạng mật mã đối xứng, như DES. Vì vậy, trong những năm 1980, chỉ có chính phủ, quân đội và các hãng lớn mới có những máy tính đủ mạnh để chạy RSA. Vì vậy không có gì đáng ngạc nhiên khi mà Công ty An toàn Dữ liệu RSA, một công ty thực hiện việc thương mại hóa RSA, đã chủ tâm phát triển các sản phẩm mã hóa của họ chỉ cho các thị trường này.

Ngược lại, Zimmermann tin rằng mọi người đều xứng đáng có quyền được riêng tư nhờ mã hóa bằng RSA và ông hướng nhiệt huyết chính trị của mình tới việc phát triển một sản phẩm mã hóa RSA đại chúng. Ông dự định sử dụng kiến thức về tin học của mình để thiết kế một sản phẩm vừa tiết kiệm vừa hiệu quả mà không gây quá tải về dung lượng cho một máy tính cá nhân bình thường. Ông cũng muốn sản phẩm RSA của ông phải có một giao diện tiện lợi và thân thiện để người sử dụng không

cần phải là một chuyên gia về mật mã cũng vận hành được. Ông gọi dự án của mình là *Pretty Good Privacy*, hay viết tắt là PGP *(Riêng tư tốt đẹp)*. Cái tên được bắt nguồn từ *Hàng tạp phẩm tốt đẹp* của Ralph, một nhà tài trợ cho chương trình *Prairie Home Company* của Garrison Keillor - một trong những chương trình phát thanh ưa thích của Zimmermann.

Trong suốt cuối những năm 1980, làm việc tại gia ở Boulder, Colorado, Zimmermann dần dần ghép xong toàn bộ gói phần mềm mã hóa của ông. Thành công chủ yếu của ông là tăng tốc độ mã hóa RSA. Thông thường, nếu Alice muốn sử dụng RSA để mã hóa thư gửi cho Bob, cô phải tìm chìa khóa công khai của anh và sau đó lắp vào hàm số một chiều của RSA. Ngược lại, Bob giải mã thư bằng cách sử dụng chìa khóa riêng để đảo ngược hàm số một chiều RSA. Cả hai quá trình đều đòi hỏi những thao tác toán học rất lớn nên việc mã hóa và giải mã, đối với những bức thư dài, sẽ phải mất vài phút trên một máy tính cá nhân. Nếu Alice gửi đi một trăm bức thư mỗi ngày, thì cô sẽ không đủ thời gian để mã hóa từng cái một. Để tăng tốc độ mã hóa và giải mã, Zimmermann đã sử dụng một mẹo khá tinh xảo là sử dụng mã hóa RSA bất đối xứng kết hợp với mã hóa đối xứng truyền thống. Mã hóa đối xứng truyền thống có thể an toàn ngang với mã hóa bất đối xứng nhưng thực hiện nhanh hơn, song mã hóa đối xứng lại vấp phải vấn đề về phân phối chìa khóa mã, nó phải được chuyển từ người gửi đến người nhận một cách an toàn. Đây chính là chỗ mà RSA xuất hiện để giải cứu, vì có thể sử dụng RSA để mã hóa chìa khóa mã đối xứng.

Zimmermann đã hình dung ra một kịch bản như sau. Nếu Alice muốn gửi một bức thư mã hóa cho Bob, cô bắt đầu mã hóa

nó bằng một mật mã đối xứng. Zimmermann khuyến nghị sử dụng một mật mã có tên là IDEA, tương tự như DES. Để mã hóa bằng IDEA, Alice cần phải lựa chọn một chìa khóa mã, song để Bob có thể giải mã được thư, Alice bằng cách nào đó phải chuyển chìa khóa mã cho Bob. Để giải quyết vấn đề này, Alice tìm chìa khóa mã công khai RSA của Bob, và sử dụng nó để mã hóa chìa khóa mã IDEA. Vì vậy, Alice phải gửi hai thứ cho Bob: bức thư được mã hóa bằng mật mã đối xứng IDEA và chìa khóa mã của IDEA đã được mã hóa bằng mật mã RSA bất đối xứng. Ở đầu kia, Bob sử dụng chìa khóa mã riêng để giải mã chìa khóa mã của IDEA, và sau đó sử dụng chìa khóa này để giải mã thư. Việc này xem ra hơi lòng vòng song lợi thế của nó là bức thư, có thể chứa một lượng lớn thông tin, được mã hóa nhanh chóng bằng mật mã đối xứng, và chỉ có chìa khóa mã của IDEA, chứa một lượng nhỏ thông tin, là được mã hóa bằng mật mã bất đối xứng chậm hơn. Zimmermann dự định sẽ đưa sự kết hợp giữa RSA và IDEA vào sản phẩm PGP, nhưng giao diện thân thiện với người sử dụng có nghĩa là họ sẽ không phải dính dáng gì đến các chi tiết kỹ thuật cụ thể của những gì đang diễn ra.

Sau khi giải quyết được phần lớn vấn đề tốc độ, Zimmermann còn muốn kết hợp một loạt những đặc tính tiện ích khác vào PGP. Chẳng hạn, trước khi sử dụng thành phần RSA trong PGP, Alice cần tạo ra chìa khóa riêng của mình và chìa khóa công khai. Việc tạo chìa khóa mã không phải là chuyện tầm thường vì nó đòi hỏi phải tìm được một cặp số nguyên tố lớn. Tuy nhiên, Alice chỉ việc ngọ nguậy chuột theo một cách bất kỳ nào đó và chương trình PGP sẽ tiến hành tạo chìa khóa riêng và chìa khóa công khai cho cô - sự di chuyển của chuột tạo ra một nhân tố

ngẫu nhiên mà PGP tận dụng để đảm bảo mỗi người sử dụng có một cặp số nguyên tố riêng, và vì vậy chìa khóa công khai và chìa khóa riêng của họ là duy nhất. Sau đó Alice chỉ việc công bố chìa khóa mã công khai của mình.

Một khía cạnh hữu dụng khác của PGP đó là khả năng ký tên một thư điện tử bằng kỹ thuật số. Thông thường thư điện tử không có chữ ký, có nghĩa là không thể xác định được tác giả thực của nó. Chẳng hạn, nếu Alice sử dụng thư điện tử để gửi một bức thư tình cho Bob, thường thì cô sẽ mã hóa nó bằng chìa khóa công khai của anh ta và khi anh nhận được thư thì giải mã bằng chìa khóa riêng. Bob lúc đầu rất sung sướng song làm thế nào có thể biết chắc chắn rằng đấy là thư tình của Alice? Có thể Eve ác tâm gửi thư và gõ tên Alice ở bên dưới thì sao. Không có sự đảm bảo bằng một chữ ký viết tay bằng mực, thì không có cách rõ ràng nào xác định được tác giả của nó. Nói cách khác, hãy tưởng tượng một ngân hàng nhận được thư điện tử của một khách hàng, trong đó yêu cầu toàn bộ tiền của mình phải được chuyển sang một tài khoản riêng ở đảo Cayman. Một lần nữa, không có chữ ký bằng tay, làm thế nào ngân hàng biết được thư điện tử đó có phải thực sự là của khách hàng hay không? Rất có thể thư điện tử này được viết bởi một tên tội phạm muốn chuyển tiền tới tài khoản ngân hàng của hắn ở đảo Cayman. Để thiết lập độ tin cậy trên Internet, cần thiết phải có một dạng chữ ký số hóa đáng tin cậy.

Chữ ký số hóa PGP dựa trên một nguyên lý do Whitfield Diffie và Martin Hellman phát hiện lần đầu tiên. Khi đề xuất ý tưởng về chìa khóa công khai và chìa khóa riêng tách biệt nhau, họ cũng nhận thấy rằng, ngoài việc giải quyết được vấn đề phân

phối chìa khóa mã, phát minh của họ cũng đưa ra một cơ chế tự nhiên cho việc tạo chữ ký thư điện tử. Trong Chương 6, chúng ta đã thấy chìa khóa công khai là để mã hóa và chìa khóa riêng là để giải mã. Trong thực tế, quá trình này có thể hoán đổi cho nhau, cụ thể là chìa khóa riêng được sử dụng để mã hóa và chìa khóa công khai dùng để giải mã. Kiểu mã hóa này thường không được chú ý vì nó không an toàn. Nếu Alice sử dụng chìa khóa riêng để mã hóa thư gửi cho Bob, thì sau đó ai cũng có thể giải mã được nó vì ai cũng có chìa khóa công khai của Alice. Tuy nhiên, cách vận hành này lại xác định được tác giả, vì nếu Bob có thể giải mã được thư bằng cách sử dụng chìa khóa công khai của Alice thì nó phải được mã hóa bằng chìa khóa riêng của cô - chỉ Alice mới có chìa khóa riêng nên bức thư phải được gửi từ Alice.

Trong thực tế, nếu Alice muốn gửi thư tình cho Bob, cô có hai lựa chọn. Hoặc cô mã hóa thư bằng chìa khóa công khai của Bob để đảm bảo an toàn, hoặc cô mã hóa bằng chìa khóa riêng của mình để khẳng định quyền tác giả. Tuy nhiên, nếu cô kết hợp cả hai lựa chọn, cô sẽ vừa bảo đảm được an toàn vừa khẳng định được quyền tác giả. Có nhiều cách nhanh hơn để đạt được điều này, song ở đây là một cách mà Alice có thể gửi thư tình của mình. Cô bắt đầu bằng việc mã hóa thư với chìa khóa riêng, sau đó mã hóa lại lần nữa bằng chìa khóa công khai của Bob. Chúng ta có thể hình dung bức thư được bao bọc bằng một vỏ ốc mỏng manh bên trong, biểu thị việc mã hóa bằng chìa khóa mã riêng của Alice, và một vỏ ốc cứng bên ngoài, biểu thị mã hóa bằng chìa khóa công khai của Bob. Bản mật mã cuối cùng chỉ Bob mới có thể giải mã vì chỉ anh mới có chìa khóa riêng cần thiết để phá vỡ vỏ ốc cứng bên ngoài. Sau khi giải mã vỏ bên ngoài,

Bob có thể giải mã một cách dễ dàng vỏ ốc bên trong bằng cách sử dụng chìa khóa công khai của Alice - vỏ ốc bên trong không nhằm bảo vệ bức thư mà chỉ để chứng minh là bức thư do Alice gửi, chứ không phải của một kẻ mạo danh nào.

Tới giai đoạn này, việc gửi một bức thư mã hóa bằng PGP vẫn còn khá phức tạp. Mật mã IDEA được dùng để mã hóa thư, RSA được sử dụng để mã hóa chìa khóa mã của IDEA, và phải thực hiện một bước mã hóa khác nữa nếu đòi hỏi phải có chữ ký số hóa. Tuy nhiên, Zimmermann đã phát triển sản phẩm của ông theo cách mà tất cả mọi thứ đều tự động, nên Alice và Bob không phải lo lắng gì về vấn đề toán học. Để gửi thư cho Bob, Alice chỉ cần đơn giản viết thư điện tử của mình và sử dụng lựa chọn PGP từ thực đơn trên màn hình máy tính. Sau đó cô đánh vào tên của Bob, PGP sẽ tìm chìa khóa công khai của Bob và tự động thực hiện các bước mã hóa. Đồng thời, PGP cũng thực hiện trò ma mãnh cần thiết để ký tên số hóa bên dưới bức thư. Khi nhận được thư đã mã hóa, Bob sẽ sử dụng lựa chọn PGP và PGP sẽ giải mã bức thư và xác minh tác giả. Không có gì trong PGP là mới mẻ cả - Diffie và Hellman đã có ý tưởng về chữ ký số hóa và các nhà tạo mã khác cũng đã sử dụng sự kết hợp giữa mật mã đối xứng và bất đối xứng để tăng tốc độ mã hóa - song Zimmermann là người đầu tiên kết hợp tất cả trong một sản phẩm mã hóa dễ sử dụng và đủ khả năng chạy trên một máy tính cá nhân trung bình.

Vào mùa hè năm 1991, Zimmermann đã chuẩn bị khá tốt để biến PGP thành một sản phẩm hoàn thiện. Chỉ còn lại hai vấn đề, nhưng đều không phải là vấn đề kỹ thuật. Một vấn đề lâu dài, đó là RSA, cốt lõi của PGP, là một sản phẩm có bản quyền,

và luật bản quyền buộc Zimmermann phải có được giấy phép từ Công ty An toàn Dữ liệu RSA trước khi tung ra PGP. Tuy nhiên, Zimmermann quyết định tạm gạt vấn đề này qua một bên. PGP không phải là sản phẩm định dành cho các hãng kinh doanh mà chỉ cho cá nhân thôi. Ông cảm thấy rằng ông sẽ không cạnh tranh trực tiếp với Công ty An toàn Dữ liệu RSA và hy vọng là trong quá trình đó rồi thì sớm hay muộn công ty sẽ cấp cho ông giấy phép miễn phí.

Một vấn đề trước mắt và nghiêm trọng hơn đó là bản dự luật của Thượng viện Mỹ năm 1991 gồm nhiều mục về chống tội phạm trong đó có điều khoản sau: "Quốc hội quyết định là những nhà cung cấp các dịch vụ thông tin điện tử và các nhà sản xuất các thiết bị dịch vụ thông tin điện tử cần đảm bảo rằng hệ thống thông tin liên lạc vẫn cho phép chính phủ có được nội dung ở dạng thường (không mã hóa - ND) của giọng nói, dữ liệu và các thông tin khác khi được pháp luật cho phép." Thượng viện lo ngại rằng sự phát triển về công nghệ số hóa, như điện thoại cầm tay, có thể cản trở các nhà hành pháp thực hiện việc nghe lén một cách có hiệu quả. Tuy nhiên, đồng thời với việc buộc các công ty phải đảm bảo khả năng nghe lén, dự luật trên cũng còn có vẻ như đe dọa mọi hình thức mã hóa an toàn.

Một nỗ lực phối hợp giữa Công ty An toàn Dữ liệu RSA, ngành công nghiệp truyền thông, và các nhóm quyền tự do công dân yêu cầu hủy bỏ điều khoản trên, song sự đồng tâm hiệp lực đó chỉ làm cho nó tạm thời được hoãn thi hành mà thôi. Zimmermann lo sợ rằng không sớm thì muộn chính phủ cũng sẽ cố thử một lần nữa và việc cấm những sản phẩm mã hóa như PGP sẽ có hiệu lực. Ông luôn có ý định muốn bán PGP, song giờ đây ông

phải xem xét lại những lựa chọn của mình. Thay vì phải chờ đợi và mạo hiểm với việc PGP bị chính phủ cấm, ông đã quyết định rằng điều quan trọng hơn là nó đến được với mọi người trước khi quá muộn. Vào tháng Sáu năm 1991, ông đã bước một bước quyết liệt, đó là nhờ một người bạn tải PGP lên bảng thông báo của Usernet. PGP chỉ là một phần mềm nên ai cũng có thể tải về miễn phí. PGP giờ đã sẵn có thoải mái trên Internet.

Đầu tiên, PGP chỉ lan truyền giữa những người say mê mật mã. Về sau, nó được đông đảo những người say Internet tải về. Rồi các tạp chí về máy tính đưa những tin ngắn và sau đó là những bài báo dài hàng trang về hiện tượng PGP. Dần dần PGP bắt đầu lan tới mọi ngóc ngách xa xôi nhất của cộng đồng kỹ thuật số. Chẳng hạn, những nhóm hoạt động vì quyền con người khắp thế giới bắt đầu sử dụng PGP để mã hóa tài liệu của họ, để ngăn chặn thông tin không bị rơi vào tay những chế độ bị cáo buộc là lạm dụng quyền con người. Zimmermann bắt đầu nhận được nhiều thư điện tử ca ngợi sáng tạo của ông. "Có những nhóm chống đối ở Myanmar", Zimmermann kể, "đang sử dụng các trại huấn luyện trong rừng sâu. Họ nói rằng nó đã giúp khích lệ tinh thần ở đó, vì trước khi PGP xuất hiện, các tài liệu bị chặn bắt sẽ dẫn đến sự bắt bớ, tra khảo và hành hình cả gia đình". Năm 1991, vào cái ngày mà Boris Yeltsin nã pháo vào tòa nhà Quốc hội ở Mátxcơva, Zimmermann nhận được bức thư điện tử dưới đây từ một ai đó ở Latvia: "Phil, tôi muốn để ông biết rằng: mong là đừng bao giờ xảy ra, nhưng nếu chế độ độc tài thâu tóm nước Nga thì PGP của ông sẽ phổ biến khắp từ Baltic đến Viễn Đông và sẽ giúp đỡ những người thuộc chủ nghĩa dân chủ nếu cần. Xin cảm ơn ông."

Trong khi Zimmermann có đông đảo người hâm mộ trên khắp thế giới thì ở quê nhà nước Mỹ, ông lại là mục tiêu bị chỉ trích. Công ty An toàn Dữ liệu RSA quyết định không cấp phép miễn phí cho Zimmermann và rất tức giận vì bản quyền bị xâm phạm. Mặc dù Zimmermann đưa PGP thành phần mềm miễn phí, song nó có chứa hệ thống mật mã chìa khóa công khai RSA, và vì vậy Công ty An toàn Dữ liệu RSA liệt PGP vào loại "phần mềm bị cấm". Zimmermann đã lơ chuyện đó đi như việc liên quan đến một ai khác chứ không phải mình. Cuộc cãi lộn về bản quyền tiếp diễn vài năm trong suốt thời gian mà Zimmermann gặp phải một vấn đề thậm chí còn lớn hơn.

Vào tháng Hai năm 1993, hai điều tra viên chính phủ đã đến gặp Zimmermann. Sau những câu hỏi ban đầu về chuyện xâm phạm bản quyền, họ bắt đầu hỏi về những cáo buộc nghiêm trọng hơn về việc xuất khẩu một vũ khí trái phép. Vì Chính phủ Mỹ gộp cả phần mềm mã hóa vào trong khái niệm vũ khí, cùng với tên lửa, súng cối và súng máy, nên PGP không được xuất khẩu nếu không có giấy phép từ Bộ Ngoại giao Mỹ. Nói cách khác, Zimmermann bị cáo buộc là một người buôn vũ khí vì ông đã xuất khẩu PGP qua Internet. Trong hơn ba năm, Zimmermann trở thành mục tiêu của một cuộc điều tra xét xử lớn và ông còn phát hiện mình bị FBI đeo bám.

Mã hóa trên diện rộng... hay không?

Cuộc điều tra đối với Phil Zimmermann và PGP đã dấy lên một cuộc tranh luận về các khía cạnh tiêu cực và tích cực của việc mã hóa trong Thời đại Thông tin. Sự lan truyền của PGP đã kích động các nhà tạo mã, các chính trị gia, những người theo chủ nghĩa tự do công dân và các nhà hành pháp phải suy nghĩ về ý nghĩa của việc mã hóa rộng rãi. Có những người, giống như Zimmermann, tin rằng việc sử dụng rộng rãi mã hóa an toàn là một lợi ích đối với xã hội, mang lại cho các cá nhân sự riêng tư trong thông tin liên lạc số hóa của họ. Đối ngược với họ là những người tin rằng mã hóa là một sự đe dọa đối với xã hội, vì bọn tội phạm và khủng bố có thể sẽ liên lạc với nhau an toàn và thoát khỏi sự nghe lén của cảnh sát.

Cuộc tranh cãi vẫn tiếp diễn trong suốt những năm 1990, và hiện nay vẫn chưa chấm dứt. Vấn đề cơ bản đặt ra là liệu chính phủ nên hay không nên làm luật chống lại khoa học mật mã. Sự tự do về mật mã cho phép mọi người, kể cả bọn tội phạm, tự tin rằng thư điện tử của họ an toàn. Trái lại, hạn chế việc sử dụng mật mã sẽ cho phép cảnh sát theo dõi được bọn tội phạm, song nó cũng cho phép cảnh sát và mọi người khác do thám các công dân bình thường. Cuối cùng, chúng ta, thông qua chính phủ mà chúng ta bầu ra, sẽ quyết định vai trò trong tương lai của khoa học mật mã. Mục này sẽ dành để tóm tắt hai mặt của cuộc tranh cãi. Phần lớn sự thảo luận liên quan đến chính sách và các nhà làm chính sách ở Mỹ, một phần vì đây chính là quê hương của PGP, mà phần nhiều cuộc tranh cãi lấy đó làm trung tâm, và một phần vì bất kỳ chính sách nào được thông qua ở Mỹ cuối cùng cũng có ảnh hưởng đến các chính sách trên toàn cầu.

Phe chống lại việc sử dụng mã hóa rộng rãi được ủng hộ bởi các nhà hành pháp, đặt trọng tâm vào mong muốn giữ nguyên hiện trạng. Trong nhiều thập kỷ, cảnh sát trên khắp thế giới đã thực hiện việc nghe lén hợp pháp để bắt tội phạm. Chẳng hạn, ở Mỹ năm 1918, việc nghe lén đã được sử dụng để làm vô hiệu hóa các điệp viên trong thời gian chiến tranh, và trong những năm 1920, họ đã chứng minh tính hiệu quả đặt biệt trong việc kết án những người bán rượu lậu. Quan điểm cho rằng nghe lén là một công cụ cần thiết của việc thực thi pháp luật đã được khẳng định vững chắc vào cuối những năm 1960, khi FBI nhận thấy rằng tội phạm có tổ chức trở thành một mối đe dọa ngày càng lớn đối với quốc gia. Những người thi hành pháp luật gặp rất nhiều khó khăn trong việc kết tội những kẻ tình nghi vì bọn tội phạm đe dọa bất cứ ai đứng ra làm chứng chống lại chúng và vì vậy mà có luật *omerta,* tức là luật im lặng. Cảnh sát nhận thấy chỉ còn hy vọng duy nhất là thu thập thông tin từ việc nghe lén và Tòa án Tối cao đã rất tán thành lập luận này. Năm 1967, nó đã ra phán quyết là cảnh sát có thể sử dụng việc nghe lén chừng nào họ được phép của tòa án.

Hai mươi năm sau, FBI vẫn duy trì khẳng định rằng "tòa án đã phán quyết việc nghe lén là một kỹ thuật điều tra hiệu quả nhất được sử dụng bởi cơ quan thực thi pháp luật để chống lại các loại thuốc cấm, khủng bố, tội phạm bạo lực, hoạt động gián điệp, và tội phạm có tổ chức". Tuy nhiên, việc nghe lén của cảnh sát sẽ vô tác dụng nếu bọn tội phạm thực hiện việc mã hóa. Một cuộc điện thoại được thực hiện qua đường dây số hóa sẽ không là gì khác hơn một chuỗi các con số, và có thể được mã hóa bằng kỹ thuật được sử dụng để mã hóa thư điện tử. Chẳng hạn PGPfone

là một trong số các sản phẩm có khả năng mã hóa liên lạc bằng giọng nói thực hiện trên Internet.

Các nhà thực thi pháp luật lập luận rằng việc nghe lén hiệu quả là cần thiết để duy trì trật tự và pháp luật, nên sự mã hóa đó cần được hạn chế để họ có thể tiếp tục việc chặn bắt thông tin. Cảnh sát từng chạm trán với bọn tội phạm sử dụng mã hóa mạnh để tự bảo vệ. Một chuyên gia pháp luật Đức nói: "Những ngành kinh doanh nóng như buôn bán vũ khí và dược phẩm không còn được thực hiện qua điện thoại mà được tiến hành dưới hình thức mã hóa trên hệ thống dữ liệu toàn cầu." Một quan chức Nhà Trắng chỉ ra một xu hướng đáng lo ngại tương tự ở Mỹ, tuyên bố rằng "thành viên của các nhóm tội phạm có tổ chức thuộc số những người sử dụng các mật mã mạnh và hệ thống máy tính tiên tiến nhất". Chẳng hạn, các carten ở Cali bố trí việc thỏa thuận mua bán thuốc qua hệ thống liên lạc được mã hóa. Các nhà thực thi pháp luật sợ rằng Internet cùng với khoa học mật mã sẽ giúp cho bọn tội phạm liên lạc và phối hợp hoạt động, và họ đặc biệt lo lắng đến cái gọi là *Four Horsemen of the Infocalypse - Bốn Kỵ sĩ của Lời tiên tri* (Kinh thánh, chương 6 Sách Khải Huyền: Bốn kỵ sĩ được nhắc đến trong lời tiên tri của Đức Chúa, đó là Chiến tranh - Nạn đói - Dịch hạch và Cái chết, ngày nay cụm từ này được dùng để ám chỉ những vấn đề đương đại - ND) - đó là những kẻ buôn thuốc phiện, tội phạm có tổ chức, khủng bố và lạm dụng trẻ em - những nhóm sẽ được hưởng lợi nhất từ việc mã hóa.

Ngoài việc mã hóa thông tin liên lạc, bọn tội phạm và khủng bố còn mã hóa kế hoạch và sổ sách ghi chép của chúng nhằm che giấu bằng chứng. Người ta đã phát hiện thấy một số tài liệu đã

được mã hóa bằng RSA của giáo phái Aum Shinrikyo, giáo phái chịu trách nhiệm về vụ tấn công bằng khí độc vào tàu điện ngầm ở Nhật năm 1995. Ramsey Yousef, một trong những tên khủng bố có liên quan đến vụ đánh bom Trung tâm Thương mại Thế giới, đã lưu giữ các kế hoạch hành động khủng bố trong tương lai được mã hóa trong máy tính xách tay của hắn. Bên cạnh các tổ chức khủng bố quốc tế, nhiều tên tội phạm bình thường khác cũng lợi dụng việc mã hóa. Chẳng hạn, một tổ chức đánh bạc phi pháp ở Mỹ đã mã hóa sổ sách kế toán của chúng trong bốn năm. Được ủy quyền bởi Nhóm công tác về Tội phạm có tổ chức thuộc Trung tâm Thông tin Chiến lược Quốc gia, năm 1997, một nghiên cứu của Dorothy Denning và William Baugh đã ước tính rằng có 500 trường hợp phạm tội trên thế giới có liên quan đến việc mã hóa, và dự đoán rằng con số này sẽ tăng gần gấp đôi mỗi năm.

Ngoài việc giám sát trong nước, còn có những vấn đề về an ninh quốc gia. Cơ quan An ninh Quốc gia Mỹ (NSA) chịu trách nhiệm thu thập thông tin tình báo về những kẻ thù của quốc gia bằng việc giải mã thông tin liên lạc của họ. NSA điều hành một mạng lưới các trạm nghe lén trên khắp thế giới với sự hợp tác của Anh, Australia, Canada và New Zealand, cùng nhau thu thập và chia sẻ thông tin. Mạng lưới bao gồm cả các địa điểm như Cơ sở Tình báo Tín hiệu Menwith Hill ở Yorkshire, một trạm tình báo lớn nhất thế giới. Một phần công việc của Menwith Hill liên quan đến hệ thống Echelon, có khả năng theo dõi thư điện tử, fax, telex và các cuộc gọi điện thoại, tìm kiếm những từ đặc biệt. Echelon vận hành theo một từ điển gồm những từ đáng ngờ như "Hezbollah" *(một giáo phái nổi lên ở Cộng hòa Lebanon, một nước nhỏ ở Trung Đông, trong nhiều năm bị coi là nhóm chuyên khủng*

bố, đánh bom liều chết và bắt cóc - ND), "kẻ ám sát" và "Clinton" và hệ thống này đủ thông minh để nhận dạng các từ này với tốc độ hợp lý. Echelon đánh dấu những bức thư khả nghi để kiểm tra kỹ lưỡng hơn, giúp nó có thể giám sát các bức thư gửi đi từ các nhóm chính trị hay tổ chức khủng bố đặc biệt. Tuy nhiên, Echelon sẽ thực sự vô dụng nếu tất cả thư từ được mã hóa bằng mật mã mạnh. Khi đó, mỗi quốc gia tham gia vào Echelon sẽ mất các thông tin tình báo có giá trị về các âm mưu chính trị và các vụ tấn công khủng bố.

Ở bên kia chiến tuyến của cuộc tranh cãi là những người theo chủ nghĩa tự do công dân, bao gồm các nhóm như Trung tâm Công nghệ và Dân chủ, và Quỹ Biên giới điện tử. Phía ủng hộ mã hóa dựa trên sự tin tưởng rằng riêng tư là một quyền cơ bản của con người, như đã được khẳng định trong Điều 12 Tuyên ngôn Chung về Quyền con người: "Không ai phải là đối tượng của sự can thiệp tùy tiện vào đời sống riêng tư, vào gia đình, nhà ở hay thư từ, cũng như sự xâm phạm đến danh dự, thanh danh của mình. Mọi người đều có quyền được pháp luật bảo vệ trước những can thiệp và xâm phạm đó".

Những người theo chủ nghĩa tự do công dân cho rằng việc sử dụng rộng rãi mã hóa là cần thiết để bảo vệ quyền được riêng tư. Nếu không, họ sợ rằng với sự phát triển của công nghệ số hóa, việc kiểm soát sẽ dễ dàng hơn nhiều, sẽ tạo ra một kỷ nguyên mới của việc đặt máy nghe lén và lạm dụng xu hướng tất yếu đó. Trong quá khứ, các chính phủ thường sử dụng quyền lực của mình để thực hiện việc nghe lén đối với cả các công dân vô tội. Tổng thống Lyndon Johnson và Richard Nixon đã phạm tội nghe trộm phi pháp và Tổng thống John F. Kenedy đã cho thực

hiện việc nghe lén đáng ngờ trong tháng đầu tiên làm tổng thống. Trong lúc chuẩn bị cho dự luật liên quan đến nhập khẩu đường từ Doninica, Kenedy đã yêu cầu đặt máy nghe trộm đối với một số nghị sĩ. Ông biện hộ là ông tin rằng họ đã bị mua chuộc, một mối lo cho an ninh quốc gia dường như rất có cơ sở. Tuy nhiên, người ta đã không tìm thấy bằng chứng nào về sự hối lộ và việc nghe lén chỉ cung cấp cho Kenedy những thông tin chính trị có giá trị, giúp cho chính quyền thông qua dự luật.

Một trong những vụ việc nổi tiếng nhất về nghe lén phi pháp liên tục có liên quan đến Martin Luther King Jr, trong đó các cuộc nói chuyện qua điện thoại của ông đã bị kiểm soát trong vài năm. Chẳng hạn, vào năm 1963, FBI đã có được thông tin về King qua một máy nghe lén và cung cấp cho Thượng nghị sĩ James Eastland để giúp ông ta tranh luận về một dự luật về quyền công dân. Thông thường hơn, FBI còn thu thập những chi tiết về cuộc sống riêng tư của King để sử dụng làm mất uy tín của ông. Những băng ghi âm về những chuyện tình ái của ông đã được gửi cho vợ ông và được bật lên trước mặt Tổng thống Johnson. Sau đó, khi King được trao giải Nobel, các chi tiết đáng xấu hổ về King đã được gửi đến mọi tổ chức có ý định trao tặng vinh dự đó cho ông.

Các chính phủ khác cũng có hành vi lạm dụng việc nghe lén tương tự. Uy ban giám sát quốc gia về chặn bắt thông tin an ninh ước tính có khoảng 100.000 vụ việc nghe lén được thực hiện ở Pháp mỗi năm. Có lẽ sự xâm phạm đến đời sống riêng tư của con người lớn nhất là chương trình Echelon quốc tế. Echelon không cần phải bào chữa cho hành động chặn bắt của mình và nó cũng không tập trung vào các cá nhân cụ thể nào. Thay vào đó, nó gặt

hái thông tin một cách không phân biệt, sử dụng các máy thu để dò thông tin phát ra từ các vệ tinh. Nếu Alice gửi một bức thư vô hại vượt Đại Tây dương đến cho Bob thì chắc chắn là nó sẽ bị Echelon chặn bắt và nếu bức thư vô tình có chứa một vài từ có trong từ điển của Echelon thì nó sẽ bị đánh dấu để kiểm tra kỹ lưỡng hơn, cùng với những thư từ của các nhóm chính trị cực đoan và các băng nhóm khủng bố. Trong khi các nhà thực thi pháp luật tranh luận rằng mã hóa cần phải bị ngăn cấm vì nó sẽ làm mất hiệu quả của Echelon, thì các nhà tự do lại cho rằng mã hóa là cần thiết chính xác là vì nó sẽ làm vô hiệu Echelon.

Khi các nhà hành pháp biện luận rằng mã hóa mạnh sẽ làm giảm đi bằng chứng kết tội bọn tội phạm, thì các nhà tự do đáp lại rằng vấn đề riêng tư là quan trọng hơn. Trong mọi trường hợp, các nhà tự do khăng khăng rằng mã hóa sẽ không phải là một rào cản lớn đối với việc thi hành luật pháp vì nghe lén không phải là công cụ chủ yếu trong hầu hết các trường hợp. Chẳng hạn, ở Mỹ năm 1994, có khoảng 1.000 vụ nghe lén được tòa án thừa nhận so với tổng số 25.000 vụ.

Không có gì đáng ngạc nhiên khi trong số những người ủng hộ cho việc tự do hóa mật mã lại có một số nhà phát minh ra mật mã chìa khóa công khai. Whitfield Diffie tuyên bố rằng các cá nhân đã được hưởng sự riêng tư trọn vẹn nhất trong lịch sử:

> Trong những năm 1970, khi Luật về các quyền được phê chuẩn, hai người bất kỳ nào cũng có thể đối thoại một cách riêng tư - mà chắc chắn là không ai trên thế giới này ngày nay còn được hưởng - bằng cách bước vài mét xuống đường và nhìn quanh để chắc không có ai nấp sau những bụi cây. Không có thiết bị

ghi âm, microphone, hay các giao thoa kế laser phát ra từ kính đeo mắt. Bạn thấy đấy, nền văn minh vẫn tồn tại. Nhiều người trong chúng ta coi thời kỳ đó là thời đại vàng của nền văn hóa chính trị Mỹ.

Ron Rivest, một trong các nhà phát minh ra RSA, cho rằng việc hạn chế mật mã là điên rồ:

> Thật là một chính sách đáng thương hại nhằm kìm kẹp một cách không phân biệt đối với một công nghệ chỉ bởi vì bọn tội phạm nào đó có thể dùng nó để giành lợi thế. Ví dụ, bất kỳ công dân Mỹ nào đều có thể tự do mua một đôi găng tay, cho dù một tên trộm có thể sử dụng nó để cướp của mà không để lại dấu vân tay. Khoa học mật mã là một công nghệ bảo vệ dữ liệu, cũng như găng tay là một công nghệ bảo vệ tay. Khoa học mật mã bảo vệ dữ liệu chống lại những kẻ ăn cắp thông tin, những điệp viên, và những nghệ sĩ lừa bịp, trong khi găng tay bảo vệ tay khỏi bị cắt, dập, nóng, lạnh và nhiễm trùng. Cái trước có thể làm hỏng việc nghe lén của FBI còn cái sau có thể cản trở FBI phân tích dấu vân tay. Khoa học mật mã và găng tay đều rẻ như bèo và đều sẵn có ở mọi nơi. Trong thực tế, bạn có thể tải về một phần mềm mật mã tốt từ Internet với giá thấp hơn một đôi găng tay xịn.

Có lẽ những Đồng minh vĩ đại nhất trong cuộc chiến của những người tự do chính là những tập đoàn lớn. Thương mại trên Internet vẫn còn trong thời kỳ phôi thai song sự buôn bán đang ngày càng phát triển với tốc độ nhanh chóng, mà đi đầu là việc bán lẻ sách, đĩa nhạc và phần mềm máy tính. Năm 1998, một triệu người Anh đã sử dụng Internet để mua các sản phẩm với

tổng giá trị là 600 triệu đôla, và đến năm 1999 đạt gấp 4 lần. Chỉ trong vài năm tới, thương mại Internet sẽ thống trị thị trường, song chỉ khi các hãng có thể giải quyết được vấn đề an toàn và sự tin cậy. Một hãng phải bảo đảm được những bí mật riêng tư và an toàn cho các giao dịch thương mại, và cách duy nhất làm được điều này là sử dụng mã hóa mạnh.

Lúc này, việc mua bán trên Internet có thể được đảm bảo bởi mật mã chìa khóa công khai. Alice vào xem trang Web của một công ty và lựa chọn một sản phẩm. Sau đó cô điền vào một mẫu đơn đặt hàng trong đó yêu cầu cô phải khai tên, địa chỉ và các chi tiết về thẻ tín dụng. Alice sau đó sử dụng chìa khóa công khai của công ty để mã hóa mẫu đặt hàng. Đơn đặt hàng được mã hóa sẽ được chuyển đến cho công ty, và chỉ có họ mới có thể giải mã vì họ có chìa khóa riêng cần thiết cho việc giải mã. Tất cả việc này được thực hiện tự động bởi trình duyệt Web của Alice (ví dụ như Netscape hay Explorer) liên kết với máy tính của công ty.

Thông thường, độ an toàn của việc mã hóa phụ thuộc vào kích thước của chìa khóa mã. Ở Mỹ, không có sự hạn chế về kích thước chìa khóa mã song các công ty phần mềm Mỹ vẫn chưa được phép xuất khẩu các sản phẩm Web có mã hóa mạnh. Vì vậy, các trình duyệt đã được xuất khẩu sang phần còn lại của thế giới chỉ có thể xử lý được các chìa khóa mã ngắn, và do đó chỉ mang lại độ an toàn trung bình. Trong thực tế, nếu Alice ở London muốn mua sách của một công ty ở Chicago, thì giao dịch qua Internet của cô ít an toàn hơn khoảng 1 tỉ tỉ tỉ lần so với giao dịch của Bob ở New York khi mua sách của cùng công ty. Giao dịch của Bob là an toàn tuyệt đối vì trình duyệt của anh hỗ trợ việc mã hóa với chìa khóa mã lớn hơn trong khi giao dịch của

Alice có thể bị giải mã bởi một tên tội phạm nào đó. May mắn là chi phí của thiết bị cần để giải mã các chi tiết thẻ tín dụng của Alice lớn hơn rất nhiều giá trị giới hạn trên thẻ tín dụng thông thường nên nó không hiệu quả về chi phí. Tuy nhiên, khi lượng tiền chảy qua Internet tăng lên thì cuối cùng nó sẽ trở nên có lợi với bọn tội phạm khi giải mã được chi tiết các thẻ tín dụng. Nói gọn lại, thì nếu thương mại Internet bị de dọa thì người tiêu dùng trên khắp thế giới sẽ phải có được độ an toàn thích hợp và các hãng sẽ không chấp nhận thứ mã hóa què quặt.

Các hãng cũng mong muốn mã hóa mạnh vì một lý do khác. Các tập đoàn lưu trữ lượng thông tin cực lớn trên cơ sở dữ liệu của máy tính bao gồm các bản mô tả sản phẩm, những chi tiết về khách hàng và sổ sách kinh doanh. Lẽ tự nhiên là các tập đoàn này muốn bảo vệ các thông tin đó, không muốn bị bọn tin tặc tấn công, xâm nhập vào máy tính và đánh cắp thông tin. Sự bảo vệ có thể thực hiện được bằng cách mã hóa các thông tin lưu trữ, nhờ đó chỉ các nhân viên có chìa khóa giải mã mới có thể truy cập được.

Tóm lại, rõ ràng đây là cuộc chiến giữa hai phe: những người tự do và các hãng ủng hộ mã hóa mạnh trong khi các nhà hành pháp lại ủng hộ việc hạn chế gắt gao. Nói chung, ý kiến đa số dường như ngả về liên minh ủng hộ mã hóa, được hậu thuẫn bởi sự đồng tình của giới truyền thông và một số phim của Hollywood. Vào đầu năm 1998, bộ phim *Mercury Rising* là câu chuyện về một mật mã mới được coi là không thể phá nổi của NSA, nhưng đã được giải mã một cách tình cờ bởi một cậu bé thần đồng 9 tuổi mắc chứng tự kỷ. Alec Baldwin, một điệp viên của NSA, được cử đi ám sát cậu bé, người đang là mối đe dọa đối với an ninh quốc

gia. May mắn là cậu bé được Bruce Willis bảo vệ. Cũng trong năm 1998, Hollywood trình làng bộ phim *Enemy of the State*, kể về một âm mưu của NSA nhằm hãm hại một chính trị gia, người đồng tình với dự luật ủng hộ mã hóa mạnh. Chính trị gia đó bị giết song một luật sư do Will Smith đóng và một người nổi loạn của NSA do Gene Hackman đóng cuối cùng đã đưa được tên ám sát của NSA ra pháp luật. Cả hai phim đều mô tả NSA tàn ác hơn cả CIA, và trên nhiều phương diện NSA đều lãnh vai trò là một mối đe dọa đầy quyền lực.

Trong khi nhóm người vận động ủng hộ mã hóa biện minh cho việc tự do mã hóa và nhóm phản đối mã hóa lại muốn hạn chế thì có một lựa chọn thứ ba, mang tính thỏa hiệp. Hơn một thập kỷ qua, các nhà tạo mã và những nhà làm chính sách đã nghiên cứu kỹ mặt thuận và chưa thuận của một kế hoạch có tên là *giao kèo chìa khóa*. Từ "giao kèo" thường liên quan đến một thỏa thuận trong đó một người đưa một khoản tiền cho bên thứ ba, người này sau đó sẽ chuyển tiền cho bên thứ hai với những điều kiện nhất định. Ví dụ, người thuê nhà có thể gửi luật sư một khoản ký thác, người này sau đó có thể chuyển cho chủ nhà trong trường hợp tài sản bị hư hỏng. Trên phương diện mật mã, giao kèo có nghĩa là Alice sẽ đưa bản sao chìa khóa mã riêng của mình cho đại lý giao kèo, một người trung gian độc lập và đáng tin cậy, người này được ủy quyền giao chìa khóa mã riêng cho cảnh sát nếu có bằng chứng đầy đủ cho thấy Alice có liên quan đến tội phạm.

Việc thử nghiệm giao kèo chìa khóa mã nổi tiếng nhất đó là Tiêu chuẩn mã hóa giao kèo của Mỹ, được thông qua năm 1994. Mục đích là để khuyến khích sử dụng hai hệ thống mã hóa, được

gọi là *clipper* và *capstone*, tương ứng cho liên lạc bằng điện thoại và liên lạc bằng máy tính. Để sử dụng mã hóa clipper, Alice sẽ phải mua máy điện thoại và một con chíp đã được cài đặt trước để giữ bí mật thông tin về chìa khóa mã riêng của cô, một bản sao của chìa khóa riêng trong con chíp sẽ được chia làm hai phần, mỗi phần được gửi đến hai cơ quan Liên bang khác nhau lưu giữ. Chính phủ Hoa kỳ cho rằng Alice sẽ có được mã hóa an toàn, và sự riêng tư của cô chỉ bị phá vỡ nếu các nhà hành pháp có thể thuyết phục được cả hai cơ quan Liên bang đó rằng có một vụ việc cần dùng đến chìa khóa mã giao kèo của cô.

Chính phủ Hoa Kỳ cũng sử dụng clipper và capstone cho chính những thông tin liên lạc của mình, và buộc các công ty có liên quan đến công việc của chính phủ phải chấp nhận Tiêu chuẩn mã hóa giao kèo của Mỹ. Những hãng khác và các cá nhân được tự do sử dụng các dạng mã hóa khác, song chính phủ hy vọng rằng clipper và capstone sẽ dần trở thành một dạng mã hóa được ưa thích khắp cả nước. Tuy nhiên, chính sách này đã không thực hiện được. Ý tưởng về giao kèo chìa khóa mã chỉ thu được vài sự ủng hộ bên ngoài chính phủ. Những người theo chủ nghĩa tự do công dân không thích ý tưởng các cơ quan Liên bang sở hữu chìa khóa mã của tất cả mọi người - họ so sánh nó với chìa khóa thông thường và hỏi lại rằng người ta sẽ cảm thấy như thế nào nếu chính phủ có chìa khóa vào cửa tất cả các ngôi nhà. Các chuyên gia mã hóa chỉ ra rằng chỉ cần một nhân viên không thật thà cũng có thể ngầm hủy hoại toàn bộ hệ thống bằng cách bán chìa khóa mã giao kèo cho người trả giá cao nhất. Và các hãng lo ngại về độ tin cậy. Chẳng hạn, một hãng châu Âu ở Mỹ có thể sợ rằng thư từ của họ sẽ bị chặn bắt bởi các quan chức thương

mại Mỹ nhằm có được những bí mật có thể đưa những đối thủ của Mỹ đến bờ vực cạnh tranh.

Mặc cho sự thất bại của clipper và capstone, rất nhiều chính phủ vẫn cố thuyết phục rằng giao kèo chìa khóa mã là có thể vận hành được, chừng nào chìa khóa mã vẫn được bảo vệ đủ tốt đối với bọn tội phạm và chừng nào vẫn có sự bảo vệ bảo đảm với công chúng rằng hệ thống không bị chính phủ lạm dụng. Louis J. Freeh, Giám đốc FBI, năm 1996 đã nói: "Phía các nhà hành pháp sẽ luôn ủng hộ đầy đủ cho một chính sách mã hóa cân bằng... Giao kèo chìa khóa mã không chỉ là một giải pháp duy nhất, mà trong thực tế, nó còn là giải pháp tốt vì nó thực sự cân bằng những mối lo ngại cơ bản của xã hội liên quan đến bí mật riêng tư, an toàn thông tin, thương mại điện tử, an toàn công cộng, và an ninh quốc gia". Mặc dù chính phủ Hoa Kỳ đã rút lại các đề xuất liên quan đến giao kèo, song rất nhiều người nghi ngại rằng sớm muộn gì rồi nó cũng sẽ cố đưa ra một dạng giao kèo chìa khóa mã khác vào một lúc nào đó trong tương lai. Trong khi đó, nhóm ủng hộ mã hóa tiếp tục đấu tranh chống lại giao kèo chìa khóa mã. Kenneth Neil Cukier, một nhà báo về công nghệ đã viết rằng: "Tất cả những người liên quan trong cuộc tranh luận về mật mã đều rất thông minh, trọng danh dự và ủng hộ cho giao kèo, song họ sẽ không bao giờ sở hữu hơn hai trong ba thứ đó cùng một lúc."

Có nhiều lựa chọn khác mà các chính phủ có thể chọn để thực hiện, nhằm cố gắng cân bằng những mối lo ngại của những người theo chủ nghĩa tự do công dân, các hãng kinh doanh và các nhà hành pháp. Cũng chưa rõ ràng là lựa chọn nào sẽ được ưa thích hơn, vì hiện tại chính sách mật mã đang ở trong trạng

thái thay đổi liên tục. Một dòng chảy ổn định các sự kiện trên khắp thế giới đang ảnh hưởng liên tục đến cuộc tranh cãi về mã hóa. Tháng Mười một năm 1998, bài nói của Nữ hoàng đã thông báo về pháp luật của nước Anh đối với lĩnh vực kỹ thuật số. Tháng Mười hai năm 1998, ba mươi ba quốc gia đã ký Hiệp ước Wassenaar về hạn chế xuất khẩu vũ khí, trong đó bao hàm cả các công nghệ mã hóa mạnh. Tháng Một năm 1999, Pháp đã bãi bỏ các luật chống mã hóa của mình, mặc dù trước đó là một nước hạn chế nhất ở Tây Âu. Đó có thể là kết quả của sức ép từ giới kinh doanh. Tháng Ba năm 1999, Chính phủ Anh cho ra mắt một tài liệu tham khảo về một dự luật Thương mại điện tử.

Cho đến lúc bạn đang đọc những dòng này thì sẽ có thêm một số những lắt léo nữa trong cuộc chiến về chính sách mật mã. Tuy nhiên, một khía cạnh có thể chắc chắn của chính sách mã hóa trong tương lai chính là sự cần thiết của *các cơ quan xác nhận*. Nếu Alice muốn gửi một thư điện tử an toàn cho một người bạn mới, Zak, cô cần phải có chìa khóa công khai của Zak. Cô có thể yêu cầu Zak gửi chìa khóa công khai cho cô qua thư. Không may là có thể có rủi ro là Eve bắt được thư của Zak gửi cho Alice, rồi hủy nó đi và giả mạo một bức thư mới, trong đó có chứa chìa khóa công khai của chính cô ta chứ không phải của Zak. Alice sau đó có thể gửi một bức thư điện tử nhạy cảm cho Zak, nhưng do không biết cô mã hóa nó bằng chìa khóa công khai của Eve. Nếu Eve chặn được lá thư này, cô ta có thể dễ dàng giải mã và đọc nó. Nói cách khác, một trong những vấn đề của mật mã chìa khóa công khai đó là phải đảm bảo rằng bạn có chìa khóa mã công khai đích thực của người mà bạn định liên lạc. Các cơ quan xác nhận là những tổ chức có nhiệm vụ xác định

một chìa khóa công khai có thực sự thuộc về một người cụ thể không. Cơ quan xác nhận này có thể yêu cầu một cuộc gặp trực tiếp với Zak như là một cách để đảm bảo rằng họ lưu giữ chính xác chìa khóa mã của anh. Nếu Alice tin tưởng vào cơ quan xác nhận, cô có thể có được chìa khóa công khai của Zak và có thể tin tưởng chìa khóa đó là thật.

Ở trên tôi đã giải thích cách thức mà Alice có thể mua hàng hóa một cách an toàn từ Internet nhờ sử dụng chìa khóa công khai của công ty để mã hóa đơn đặt hàng. Trong thực tế, cô sẽ chỉ làm việc này nếu chìa khóa công khai đó đã được chứng thực bởi một cơ quan xác nhận. Năm 1998, dẫn đầu thị trường về xác nhận là Verisign, một công ty đã tăng trưởng tới 30 triệu đôla chỉ trong bốn năm. Cùng với sự đảm bảo mã hóa đáng tin cậy bằng việc xác nhận chìa khóa mã công khai, các cơ quan chứng nhận cũng có thể đảm bảo cả tính hợp lệ của chữ ký số hóa. Năm 1998, hãng Baltimore Technologies ở Ireland đã xác nhận chữ ký số hóa của Tổng thống Bill Clinton và Thủ tướng Bertie Ahern. Điều này cho phép hai vị lãnh đạo đó ký bằng kỹ thuật số vào một bản thông cáo chung ở Dublin.

Các cơ quan xác nhận không gây rủi ro gì cho sự an toàn. Họ đơn giản chỉ yêu cầu Zak tiết lộ chìa khóa công khai của anh để họ có thể chứng thực nó cho người khác, những người muốn gửi thư đã mã hóa cho anh. Tuy nhiên, có các công ty khác, được gọi là *bên thứ ba tin cậy* (TTP), lại cung cấp một một dịch vụ còn gây bàn cãi hơn nữa, gọi là *khôi phục chìa khóa mã*. Hãy tưởng tượng một hãng luật bảo vệ tất cả các tài liệu có tầm quan trọng sống còn bằng cách mã hóa chúng nhờ chìa khóa công khai của riêng họ, do vậy chỉ có họ mới giải mã được bằng chìa khóa riêng. Một

hệ thống như vậy là một biện pháp hiệu quả chống lại bọn tin tặc và bất cứ ai khác cố ý đánh cắp thông tin. Tuy nhiên, điều gì sẽ xảy ra nếu nhân viên, người giữ chìa khóa mã riêng lại quên mất nó, bỏ trốn cùng nó hoặc bị tai nạn giao thông? Các chính phủ đang khuyến khích lập các TTP để giữ bản sao của tất cả các chìa khóa mã. Một công ty nào bị mất chìa khóa mã riêng đều có thể khôi phục lại được bằng cách tiếp cận TTP của nó.

Bên thứ ba tin cậy là điều gây tranh cãi bởi vì họ có thể tiếp cận được với chìa khóa riêng của mọi người, và do đó họ có khả năng đọc được thư tín của các khách hàng của mình. Họ phải thực sự đáng tin cậy, nếu không hệ thống rất dễ dàng bị lạm dụng. Một số người cho rằng TTP chính là hiện thân của giao kèo, và rằng các nhà hành pháp dễ bị cám dỗ bắt buộc các TTP phải tiết lộ các chìa khóa mã riêng của khách hàng trong quá trình điều tra của cảnh sát. Những người khác thì vẫn cho rằng TTP là một bộ phận cần thiết của một cơ sở hạ tầng chìa khóa mã hợp lý.

Không ai có thể dự đoán được vai trò của TTP trong tương lai, và không ai có thể đoán trước một cách chắc chắn chính sách mật mã sẽ ra sao sau 10 năm nữa. Tuy nhiên, tôi ngờ rằng trong tương lai gần, phe ủng hộ mã hóa sẽ thắng bước đầu trong cuộc tranh cãi, chủ yếu là bởi vì không quốc gia nào lại muốn có các quy định về mã hóa ngăn cấm thương mại điện tử. Tuy nhiên, nếu chính sách này hóa ra là sai lầm thì luôn có thể đảo ngược lại luật. Nếu có một loạt những hành động bạo lực khủng bố và các nhà hành pháp có thể chứng minh được rằng việc nghe lén sẽ ngăn chặn được chúng thì các chính phủ sẽ nhanh chóng có được sự đồng tình với chính sách giao kèo chìa khóa mã. Tất cả những người sử dụng mã hóa mạnh sẽ bị buộc phải gửi chìa khóa

mã của mình vào một đại lý giao kèo, và sau đó những ai gửi thư mã hóa bằng một chìa khóa mã không giao kèo sẽ là phạm luật. Nếu việc xử phạt hành động mã hóa không giao kèo là đủ nghiêm khắc thì các nhà hành pháp có thể lấy lại quyền kiểm soát. Sau này, nếu chính phủ định lạm dụng độ tin cậy của hệ thống giao kèo chìa khóa mã thì công chúng sẽ đòi hỏi tự do mã hóa trở lại và con lắc sẽ lệch về hướng ngược lại. Nói tóm lại, không có lý do gì mà chúng ta không thể thay đổi chính sách của mình cho phù hợp với môi trường chính trị, kinh tế và xã hội. Nhân tố quyết định sẽ là người mà xã hội lo sợ nhất - tội phạm hay chính phủ.

Sự phục hồi của Zimmermann

Năm 1993, Phil Zimmermann trở thành đối tượng của một cuộc điều tra lớn. Theo FBI, ông đã xuất khẩu một loại vũ khí vì ông đã cung cấp cho các quốc gia thù địch và bọn khủng bố những công cụ mà chúng cần để phá hoại quyền lực của Chính phủ Hoa Kỳ. Khi cuộc điều tra kéo dài, ngày càng nhiều các nhà tạo mã và những người theo chủ nghĩa tự do đổ xô vào ủng hộ cho Zimmermann, lập nên một quỹ quốc tế hỗ trợ về tài chính để bào chữa cho ông. Đồng thời, tiếng tăm của việc trở thành đối tượng truy nã của FBI đã càng làm tăng danh tiếng của PGP, và sáng tạo của Zimmermann ngày càng lan rộng nhanh chóng qua Internet - cuối cùng thì nó chính là phần mềm mã hóa an toàn đến mức đe dọa cả đến Liên bang.

Riêng tư tốt đẹp ban đầu được công bố vội vàng và vì vậy nó chưa phải là một sản phẩm hoàn thiện như nó có thể. Ngay lập tức đã có làn sóng đòi hỏi phải phát triển phiên bản PGP cải tiến,

song rõ ràng là Zimmermann không thể tiếp tục công việc này được nữa. Thay vào đó, các kỹ sư phần mềm ở châu Âu bắt đầu công việc xây dựng lại PGP. Nói chung, thái độ của châu Âu đối với việc mã hóa là thoáng hơn và đến nay vẫn vậy, không có hạn chế nào đối với việc xuất khẩu một hệ PGP châu Âu đi khắp thế giới. Hơn nữa, cuộc cãi lộn về bản quyền của RSA không phải là một vấn đề ở châu Âu vì bản quyền đối với RSA không có hiệu lực bên ngoài nước Mỹ.

Sau ba năm, cuộc điều tra lớn vẫn không đưa được Zimmermann ra xét xử. Vụ việc phức tạp là do bản chất của PGP và cách thức mà nó được tạo dựng. Nếu Zimmermann cài PGP vào máy tính và sau đó vận chuyển nó cho một chính quyền thù địch thì vụ việc chống lại ông đã đơn giản, vì rõ ràng là ông phạm tội xuất khẩu một hệ thống mã hóa vận hành hoàn hảo. Tương tự như vậy, nếu ông đã xuất khẩu một đĩa có chứa chương trình PGP, thì đồ vật hữu hình đó có thể biểu thị cho một thiết bị mã hóa, và một lần nữa tội của Zimmermann sẽ là chắc chắn. Trái lại, nếu ông đã in ra một chương trình máy tính và xuất khẩu nó dưới dạng sách, thì vụ việc không còn là rõ ràng nữa vì ông sẽ chỉ bị xem xét là đã xuất khẩu kiến thức chứ không phải là một thiết bị mã hóa. Tuy nhiên, nội dung in có thể dễ dàng được quét lại và thông tin được nạp trực tiếp vào một máy tính thì đồng nghĩa với việc cuốn sách đó nguy hiểm như một chiếc đĩa. Điều thực sự xảy ra là Zimmermann đã đưa một bản sao PGP cho một "người bạn", người này đơn giản là đã cài đặt nó vào một máy tính của Mỹ tình cờ đang nối mạng Internet. Như vậy thì một chính quyền thù địch có thể tải nó về hoặc có thể không. Vậy thì liệu Zimmermann đã thực sự phạm tội xuất khẩu PGP chưa?

Thậm chí ngày nay, những vấn đề pháp lý xung quanh Internet vẫn còn là chủ đề tranh cãi và còn phải làm sáng tỏ. Huống chi trở lại đầu những năm 1990, tình hình lúc đó là cực kỳ mơ hồ.

Năm 1996, sau ba năm điều tra, Văn phòng Chưởng lý Hoa kỳ đã xóa bỏ vụ việc chống lại Zimmermann. FBI nhận thấy rằng đã quá muộn - PGP đã thoát ra Internet và việc truy tố Zimmermann cũng chẳng mang lại kết quả gì. Thêm một vấn đề nữa là Zimmermann được ủng hộ bởi những tổ chức lớn như nhà xuất bản của Viện Công nghệ Massachusetts (MIT), nơi đã xuất bản PGP trong một cuốn sách dày 600 trang. Cuốn sách này được bán ra khắp thế giới vì vậy việc truy tố Zimmermann sẽ có nghĩa là truy tố nhà xuất bản MIT. FBI do dự theo đuổi vụ việc này còn bởi vì khả năng Zimmermann không bị kết án là rất lớn. Một phiên tòa xử của FBI có thể chẳng mang lại điều gì hơn là một cuộc tranh cãi đáng xấu hổ về hiến pháp liên quan đến quyền được riêng tư, do vậy lại càng khuấy động sự ủng hộ của công chúng đối với việc mã hóa rộng rãi.

Vấn đề chủ yếu khác của Zimmermann cũng không còn nữa. Vì cuối cùng ông cũng đạt được thỏa thuận với RSA và có được giấy phép, giải quyết được vấn đề về bản quyền. Rốt cuộc thì PGP đã là một sản phẩm hợp pháp và Zimmermann được tự do. Cuộc điều tra đã đưa ông vào một cuộc thập tự chinh về khoa học mật mã và tất cả các giám đốc marketing trên thế giới đều phải ghen tỵ với tiếng tăm và được công chúng biết đến rộng rãi như vụ việc đã mang lại cho PGP. Cuối năm 1997, Zimmermann đã bán PGP cho hãng Network Associates và ông trở thành một thành viên cao cấp của nó. Mặc dù PGP ngày nay được bán cho các hãng kinh doanh, nhưng nó vẫn sẵn có miễn phí cho các cá nhân có ý

định sử dụng nó cho bất kỳ mục đích thương mại nào. Nói cách khác, các cá nhân, những người chỉ mong có quyền được riêng tư, vẫn có thể tải PGP từ Internet mà không phải mất đồng nào.

Nếu bạn thích có một bản của PGP, thì có rất nhiều trang Web trên Internet cung cấp nó, và bạn sẽ tìm thấy chúng tương đối dễ dàng. Có một nguồn đáng tin cậy nhất là http://www.pgpi.com/, trang chủ của PGP quốc tế, từ đây bạn có thể tải về các hệ PGP của Mỹ và quốc tế. Ở đây, xin nói ngay là tôi sẽ không chịu một trách nhiệm nào - nếu bạn chọn cài đặt PGP, bạn phải kiểm tra máy tính của mình có khả năng chạy được nó hay không, phần mềm đó có bị virus xâm nhập không, v.v... Bạn cũng nên kiểm tra xem đất nước mình đang sống có cho phép sử dụng mã hóa mạnh hay không. Và cuối cùng, bạn nên đảm bảo rằng bạn đang tải về một hệ PGP thích hợp: các cá nhân sống bên ngoài nước Mỹ không thể tải về hệ PGP của Mỹ vì như thế là xâm phạm đến luật xuất khẩu của Mỹ. Hệ PGP quốc tế thì không chịu những hạn chế xuất khẩu như vậy.

Tôi vẫn còn nhớ buổi chiều chủ nhật khi tôi tải về lần đầu tiên một bản PGP từ Internet. Từ đó tôi đã có thể bảo đảm an toàn cho các thư điện tử của mình không bị chặn bắt và đọc trộm, vì tôi giờ đây đã mã hóa tất cả những tài liệu nhạy cảm như Alice, Bob và bất kỳ ai khác sở hữu phần mềm PGP. Máy tính cá nhân của tôi và phần mềm PGP đã mang lại cho tôi độ an toàn vượt ra ngoài mọi nỗ lực kết hợp của tất cả các tổ chức giải mã trên khắp thế giới.

Bước nhảy lượng tử vào tương lai

Trong hai ngàn năm, các nhà tạo mã đã chiến đấu để bảo vệ những bí mật trong khi các nhà giải mã lại làm hết sức mình để khám phá những bí mật đó. Đây luôn là một cuộc đua ngang sức ngang tài, trong đó các nhà giải mã luôn đánh trả khi các nhà tạo mã dường như đang kiểm soát tình hình, rồi các nhà tạo mã lại phát minh ra những dạng mật mã mới mạnh hơn. Sự phát minh ra mật mã chìa khóa công khai và cuộc tranh luận mang màu sắc chính trị xung quanh việc sử dụng mã hóa mạnh là hiện trạng của ngày hôm nay và rõ ràng là các nhà tạo mã đang thắng thế trong cuộc chiến tranh thông tin. Theo Phil Zimmermann, chúng ta đang sống trong thời đại vàng của khoa mật mã: "Giờ thì trong khoa học mật mã hiện đại, có thể tạo ra những mật mã thực sự, thực sự nằm ngoài tầm với của tất cả các kỹ thuật giải mã đã biết. Và tôi cho rằng sẽ vẫn còn tiếp tục như vậy". Quan điểm của Zimmermann được sự ủng hộ của William

Crowell, Phó giám đốc của NSA: "Nếu tất cả các máy tính cá nhân trên thế giới - xấp xỉ khoảng 260 triệu máy - được kết hợp lại để xử lý một bức thư được mã hóa bằng PGP, thì sẽ phải mất một thời gian trung bình là 12 triệu lần tuổi của vũ trụ mới giải nổi chỉ một bức thư".

Tuy nhiên, kinh nghiệm trước đây cho chúng ta thấy rằng tất cả những mật mã từng được coi là không thể hóa giải nổi, sớm hay muộn gì, đều sẽ phải đầu hàng các nhà giải mã. Mật mã Vigenère còn được gọi là "mật mã không thể phá nổi", song Babbage đã phá vỡ nó; Enigma cũng được xem là không thể giải mã được cho đến khi người Ba Lan tìm ra những điểm yếu của nó. Vậy phải chăng các nhà giải mã đang đứng bên bờ của một đột phá mới, hay là Zimmermann đúng? Dự đoán sự phát triển tương lai trong bất kỳ công nghệ nào luôn là một nhiệm vụ thiếu cơ sở chắc chắn, song với mật mã thì nhiệm vụ đó còn tiềm ẩn nhiều rủi ro hơn nữa. Chúng ta không chỉ phải dự đoán những khám phá nằm trong tương lai mà còn phải dự đoán cả những khám phá ở ngay trong hiện tại. Giai thoại về James Ellis và GCHQ đã cảnh báo chúng ta rằng có thể đã có những đột phá lớn ẩn giấu sau tấm màn bí mật của chính phủ.

Chương cuối cùng này sẽ xem xét một số ý tưởng mang tính dự báo về tương lai có thể tăng cường hoặc phá vỡ những bí mật riêng tư trong thế kỷ 21. Mục tiếp sau sẽ bàn đến tương lai của việc giải mã, và đặc biệt là một ý tưởng có thể giúp cho các nhà giải mã phá vỡ tất cả các mật mã của ngày hôm nay. Ngược lại, phần cuối của cuốn sách sẽ xem xét một triển vọng lý thú nhất về mật mã, đó là hệ thống có tiềm năng bảo đảm bí mật tuyệt đối.

Tương lai của giải mã

Mặc cho sức mạnh cực lớn của RSA và các mật mã hiện đại khác, các nhà giải mã vẫn đóng một vai trò quan trọng trong việc thu thập thông tin tình báo. Thành công của họ được minh chứng bởi thực tế là nhu cầu về các nhà giải mã đang tăng cao hơn bao giờ hết - NSA vẫn là nơi sử dụng các nhà toán học nhiều nhất trên thế giới.

Chỉ có một tỷ lệ nhỏ thông tin lưu chuyển khắp thế giới là được mã hóa an toàn và phần còn lại thì được mã hóa yếu hoặc không mã hóa gì hết. Đó là vì số lượng người sử dụng Internet tăng với tốc độ chóng mặt, nhưng lại rất ít người trong số họ quan tâm đầy đủ đến vấn đề bí mật. Như vậy có nghĩa là các cơ quan an ninh quốc gia, các nhà hành pháp và bất kỳ ai khác có ý tò mò đều có thể có trong tay nhiều thông tin hơn là họ có thể đương đầu.

Ngay cả nếu người sử dụng dùng mật mã RSA một cách hợp lý thì nhà giải mã vẫn thu lượm được nhiều thứ từ những bức thư bắt được. Các nhà giải mã tiếp tục sử dụng những kỹ thuật cũ như phân tích luồng thông tin; nếu nhà giải mã không thể thăm dò được nội dung thư, thì chí ít họ cũng có thể biết được ai là người gửi và ai là người nhận mà bản thân bức thư để lộ ra. Một phát minh mới đây được gọi là tấn công bằng thiết bị bắt tín hiệu điện từ *(tempest attack)*, mà mục đích của nó là phát hiện các tín hiệu điện từ phát ra từ các thiết bị điện tử trong bộ phận hiển thị của máy tính. Nếu Eve đỗ một chiếc xe tải bên ngoài nhà Alice, cô ta có thể sử dụng thiết bị bắt tín hiệu điện từ cực nhạy để nhận dạng mỗi lần Alice gõ trên bàn phím máy tính. Điều này cho phép Eve bắt được thư ngay khi nó còn đang được gõ trên máy vi tính, trước cả khi nó được mã hóa. Để bảo vệ trước sự

tấn công bằng thiết bị bắt tín hiệu này, các công ty đã cung cấp những vật liệu che chắn dùng để phủ các bức tường phòng nhằm ngăn chặn không cho các tín hiệu điện từ thoát ra ngoài. Ở Mỹ, trước khi mua các vật liệu che chắn như vậy cần phải được phép của Chính phủ, điều này cho thấy các tổ chức như FBI thường dựa vào việc theo dõi bằng thiết bị bắt tín hiệu điện từ.

Các cách thức tấn công khác bao gồm việc sử dụng vi rút và các con ngựa thành Troy. Eve có thể thiết kế một con vi rút và cài vào phần mềm PGP và nằm yên đợi bên trong máy tính của Alice. Khi Alice sử dụng chìa khóa riêng để giải mã thư, con vi rút đó sẽ thức dậy và ghi lại chìa khóa đó. Lần sau khi Alice nối mạng Internet, vi rút này sẽ lén gửi chìa khóa riêng của Alice cho Eve, nhờ đó cô ta có thể giải mã tất cả các bức thư được gửi tới cho Alice sau đó. Con ngựa Troy, một thủ đoạn phần mềm khác, trong đó Eve thiết kế một chương trình vận hành giống như một sản phẩm mã hóa chính cống, song thực sự lại đánh lừa người sử dụng. Chẳng hạn, Alice nghĩ rằng cô đã tải về một bản sao đích thực của PGP, trong khi thực tế thì cô đã tải về một kiểu con ngựa thành Troy. Phiên bản trá hình này thoạt nhìn thì giống như chương trình PGP thật, song có chứa các lệnh để gửi bản sao văn bản thường của tất cả thư từ của Alice tới cho Eve. Như Phil Zimmermann bình luận: "Bất kỳ ai cũng có thể sửa đổi mã nguồn và tạo ra một mô phỏng PGP vô hồn như người máy, trông giống như thật song lại thực hiện mệnh lệnh của những người chủ hiểm ác. Phiên bản dạng con ngựa thành Troy này của PGP có thể được lưu hành rộng rãi, và được xem như là của tôi. Thật là xảo quyệt! Bạn cần phải tìm mọi cách để có được bản PGP từ một nguồn đáng tin cậy, theo mọi nghĩa".

Một biến thể của con ngựa thành Troy, đó là một phần mềm mã hóa mới tinh tưởng như là an toàn, nhưng thực chất lại có chứa một *cửa sau*, cho phép những người thiết kế ra nó giải mã được thư từ của tất cả mọi người. Năm 1998, một báo cáo của Wayne Madsen cho thấy công ty mật mã Thụy sĩ Crypto AG đã lắp sẵn các cửa sau vào một số sản phẩm của nó, và cung cấp cho Chính phủ Hoa Kỳ chi tiết làm thế nào để tận dụng các cửa sau này. Kết quả là Mỹ đã có thể đọc được thông tin của một số quốc gia. Năm 1991, những kẻ ám sát Shahpour Bakhtiar, nguyên thủ tướng Iran sống lưu vong, đã bị bắt là nhờ chặn bắt được và giải mã thành công các thư từ của Iran sử dụng thiết bị mã hóa của Crypto AG.

Mặc dù sự phân tích luồng thông tin, tấn công bằng các thiết bị bắt tín hiệu điện từ, vi rút và các con ngựa thành Troy đều là những kỹ thuật hữu dụng để thu thập thông tin, song các nhà giải mã hiểu rằng thành công thực sự của họ phải là tìm ra một cách để hóa giải được mật mã RSA, nền tảng của mã hóa hiện đại. Mật mã RSA được sử dụng để bảo vệ những thông tin quan trọng nhất trong quân sự, ngoại giao, thương mại và tội phạm - đó mới chính là những thông tin mà các tổ chức thu thập thông tin tình báo muốn giải mã. Nếu định thách thức mã hóa RSA mạnh, thì các nhà giải mã sẽ phải làm được một đột phá quan trọng về lý thuyết hoặc công nghệ.

Một đột phá về lý thuyết sẽ phải là một phương cách mới về cơ bản để tìm ra chìa khóa riêng của Alice. Chìa khóa riêng của Alice có chứa p và q, và chúng được tính ra bằng cách phân tích chìa khóa công khai, tức số N, ra thừa số nguyên tố. Cách tiếp cận thông thường là kiểm tra các số nguyên tố, mỗi số một lần, để xem N có chia hết cho nó hay không, song chúng ta biết rằng

làm như vậy sẽ mất rất nhiều thời gian. Các nhà giải mã đã cố gắng tìm kiếm một con đường tắt để phân tích ra thừa số, một phương pháp làm giảm một cách đáng kể số bước cần thiết để tìm ra p và q, song đến nay tất cả những nỗ lực đó đều kết thúc thất bại. Các nhà toán học đã nghiên cứu về sự phân tích ra thừa số trong nhiều thế kỷ và kỹ thuật phân tích hiện đại cũng không tốt hơn bao nhiêu so với các kỹ thuật cổ đại. Thực tế, rất có thể là các định luật toán học không cho phép tồn tại một con đường tắt đáng kể đối với việc phân tích ra thừa số cũng nên.

Không có nhiều hy vọng có một đột phá về phương diện lý thuyết, các nhà giải mã buộc phải tìm kiếm một sự đổi mới về công nghệ. Nếu không có một cách rõ ràng để giảm được số bước cần thực hiện để phân tích ra thừa số thì các nhà giải mã cần phải có một công nghệ thực hiện các bước này một cách nhanh chóng hơn. Các chíp silicon mỗi năm vẫn tiếp tục nhanh hơn, cứ 18 tháng tốc độ lại tăng khoảng gần gấp đôi, song như thế vẫn chưa đủ để có tác động thực sự đến tốc độ phân tích ra thừa số - các nhà giải mã cần một công nghệ nhanh hơn 1 tỉ lần so với các máy tính hiện tại. Do vậy, các nhà giải mã đang hướng tới một dạng máy tính hoàn toàn mới, *máy tính lượng tử*. Nếu các nhà khoa học có thể chế tạo được một máy tính lượng tử thì nó sẽ thực hiện các tính toán với tốc độ cực lớn khiến cho các siêu máy tính hiện đại chỉ còn như một cái bàn tính vỡ.

Phần còn lại của mục này sẽ bàn về khái niệm máy tính lượng tử, và do đó cũng sẽ giới thiệu một số nguyên lý của vật lý lượng tử, mà đôi khi còn gọi là cơ học lượng tử. Trước khi đi sâu hơn, xin vui lòng lưu ý một lời cảnh báo của Niels Bohr, một trong những cha đẻ của cơ học lượng tử: "Bất kỳ ai suy ngẫm về cơ học

lượng tử mà không thấy choáng váng thì sẽ không hiểu được nó". Nói cách khác, bạn hãy chuẩn bị để đón nhận một số ý tưởng khá kỳ quặc.

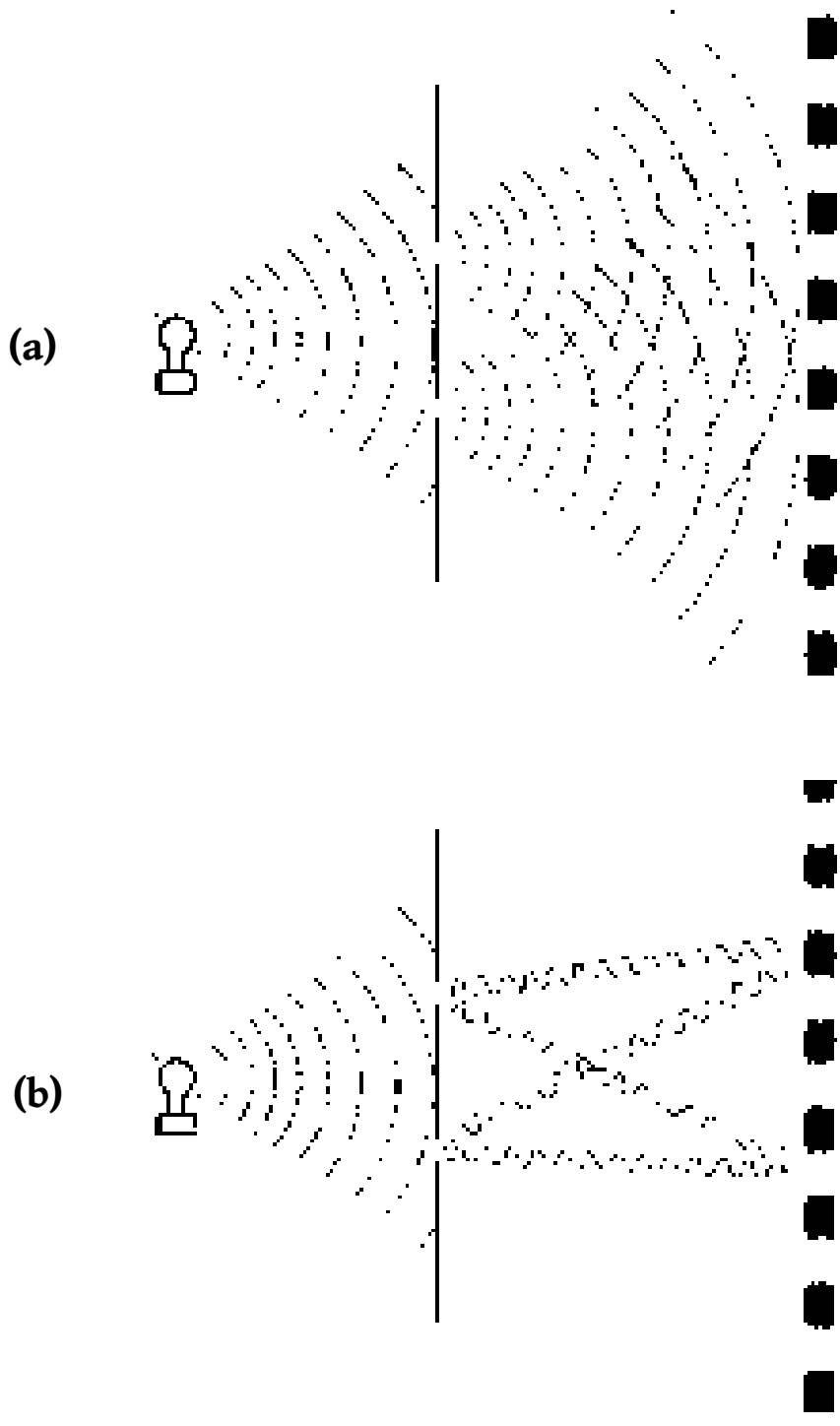
Để giải thích các nguyên lý của máy tính lượng tử, sẽ là hữu ích nếu ta quay trở lại cuối thế kỷ 18 và thành quả của Thomas Young, một tài năng nhiều mặt của nước Anh, người đã có công đột phá đầu tiên trong việc giải mã các chữ tượng hình của người Ai Cập. Là thành viên của trường Emmanuel College, Cambridge, Young thường dành những buổi chiều để thư giãn bên hồ vịt của trường. Vào một buổi chiều đặc biệt, - theo truyền thuyết kể lại, - ông chú ý thấy hai chú vịt đang bơi lội tung tăng bên nhau. Ông quan sát thấy rằng hai con vịt để lại hai vệt gợn sóng phía sau chúng, hai gợn sóng tương tác và tạo nên một bức tranh kỳ lạ gồm những vết phẳng lặng và những vết dao động mạnh xen kẽ nhau. Sở dĩ như vậy là vì, khi hai sóng xòe ra phía sau hai con vịt chồng chập lên nhau, nếu một đỉnh sóng của con vịt này chồng lên một hõm sóng của con vịt kia thì sẽ tạo nên một vệt nhỏ nước lặng yên, đỉnh và hõm đã triệt tiêu lẫn nhau. Còn nếu hai đỉnh hoặc hai hõm đến cùng một chỗ đồng thời, thì kết quả sẽ là một đỉnh cao hơn hoặc một hõm sâu hơn. Ông đặc biệt thích thú vì các chú vịt gợi ông nhớ đến một thí nghiệm liên quan đến bản chất của ánh sáng mà ông đã thực hiện năm 1799.

Trong thí nghiệm trước đây của Young, ông đã chiếu ánh sáng qua một màn chắn, trên đó có hai khe hở thẳng đứng và hẹp như trên Hình 71(a). Trên một màn ảnh đặt phía sau hai khe, Young nghĩ là sẽ thấy hai vạch sáng, hình chiếu của hai khe. Nhưng thay vì thế, ông lại thấy ánh sáng xòe ra từ hai khe và tạo nên một hình ảnh gồm một số vạch sáng và tối xen kẽ nhau trên màn ảnh.

Hình ảnh các vạch sáng và tối trên màn lúc đó đã khiến ông bối rối song giờ đây ông tin rằng ông có thể giải thích được tất cả dựa trên những gì ông thấy trên hồ vịt.

Young bắt đầu bằng việc giả sử rằng ánh sáng là một dạng sóng. Nếu ánh sáng phát ra từ hai khe hành xử như sóng thì nó cũng giống như các gợn sóng ở phía sau hai chú vịt. Hơn nữa, các vạch sáng và tối trên màn ảnh được tạo bởi cùng những tương tác như đã làm cho sóng nước tạo nên các đỉnh cao hơn, các hõm sâu hơn và các vệt phẳng lặng. Young đã hình dung ra ngay các điểm trên màn ảnh, ở đó một hõm sóng gặp một đỉnh sóng, chúng sẽ triệt tiêu lẫn nhau và tạo nên một vân tối, trong khi đó, tại những điểm trên màn ảnh mà hai đỉnh (hoặc hai hõm) sóng gặp nhau, chúng sẽ tăng cường lẫn nhau và là vân sáng như ta thấy trên Hình 71(b). Như vậy các chú vịt đã giúp Young hiểu sâu hơn bản chất thực của ánh sáng, và cuối cùng ông đã cho công bố *Thuyết sóng ánh sáng*, một trong những bài báo vật lý kinh điển của mọi thời đại.

Ngày nay, chúng ta đã biết rằng ánh sáng thực sự hành xử như một sóng, song chúng ta còn biết rằng nó cũng hành xử như một hạt. Việc ánh sáng ở dạng sóng hay dạng hạt còn tùy thuộc vào hoàn cảnh, và tình trạng nhập nhằng này của ánh sáng được gọi là lưỡng tính sóng-hạt của nó. Chúng ta không cần bàn thêm về lưỡng tính này, ngoài việc nói thêm rằng vật lý học hiện đại cho rằng một tia sáng gồm vô số các hạt riêng lẻ, được gọi là phôtôn, nhưng các hạt này lại bộc lộ những tính chất giống như sóng. Xem xét theo hướng này, chúng ta có thể diễn giải thí nghiệm của Young là do các phôtôn bay qua hai khe, và sau đó tương tác với nhau ở phía sau màn chắn có hai khe.



Hình 71 Thí nghiệm hai khe của Young được quan sát từ trên xuống. Hình (a) cho thấy ánh sáng xòe ra từ hai khe trên màn chắn tương tác với nhau và tạo nên hình ảnh các vân trên màn ảnh. Hình (b) cho thấy hai sóng tương tác với nhau như thế nào. Nếu một hõm gặp một đỉnh ở trên màn ảnh, kết quả là một vân tối. Nếu hai hõm (hoặc hai đỉnh) gặp nhau trên màn ảnh, kết quả là một vân sáng.

Cho đến đây, chưa có gì là kỳ lạ đặc biệt trong thí nghiệm của Young cả. Tuy nhiên, công nghệ hiện đại cho phép các nhà vật lý thực hiện lại thí nghiệm của Young, nhưng sử dụng một sợi tóc bóng đèn mờ đến mức nó chỉ phát ra các phôtôn ánh sáng riêng lẻ với tốc độ, chẳng hạn, một phôtôn trong một phút, và do đó mỗi lần chỉ có một phôtôn đi tới màn chắn có hai khe. Khi đó, thi thoảng lại có một phôtôn đi qua một trong hai khe và đập vào màn ảnh. Mặc dù mắt ta không đủ nhạy để thấy được từng phôtôn riêng rẽ, song chúng có thể quan sát được bằng một máy dò đặc biệt, và trong nhiều giờ đồng hồ, chúng ta có thể xác lập được một bức tranh tổng thể về những chỗ mà các phôtôn đập vào màn ảnh. Chỉ với một phôtôn mỗi lần đi qua các khe, chúng ta không nghĩ rằng sẽ lại nhìn thấy hình ảnh các vân như Young đã quan sát thấy, vì hiện tượng này dường như phụ thuộc vào hai phôtôn đồng thời đi qua hai khe và tương tác với nhau ở phía bên kia hai khe. Thay vì thế, chúng ta nghĩ là sẽ quan sát thấy hai vạch sáng, đơn giản chỉ là hình chiếu của hai khe trên màn ảnh. Tuy nhiên, vì một lý do kỳ lạ nào đó, ngay cả với các phôtôn đơn lẻ thì kết quả trên màn vẫn là hình ảnh các vân sáng và tối xen kẽ, như thể các phôtôn đã tương tác với nhau.

Kết quả kỳ lạ này thách thức lẽ phải thông thường. Không có cách nào lý giải được hiện tượng này thông qua các định luật của vật lý cổ điển, mà cụ thể là các định luật truyền thống mà chúng ta đã tìm ra để giải thích hành vi của các vật trong cuộc sống hằng ngày. Vật lý học cổ điển có thể giải thích quỹ đạo của các hành tinh hay đường đi của một viên đạn, song không thể mô tả một cách đầy đủ thế giới của những vật thực sự bé như đường đi của một phôtôn. Để giải thích hiện tượng phôtôn, các

nhà vật lý phải viện đến lý thuyết lượng tử, lý thuyết được dùng để mô tả hành vi của các vật ở cấp độ vi mô. Tuy nhiên, ngay cả các nhà lý thuyết lượng tử cũng không thể nhất trí trong việc giải thích thí nghiệm này. Họ có xu hướng tách thành hai phe đối lập nhau, mỗi phe có cách giải thích riêng của mình.

Phe thứ nhất thừa nhận một ý tưởng được gọi là *sự chồng chất*. Sự chồng chất bắt đầu bằng việc tuyên bố rằng chúng ta chỉ biết có hai điều chắc chắn về phôtôn - đó là nó đi ra từ sợi tóc bóng đèn và đập vào màn hình. Mọi thứ khác đều hoàn toàn bí ẩn, kể cả việc các phôtôn đi qua khe bên trái hay khe bên phải. Vì đường đi chính xác của phôtôn là không biết, những người đi theo thuyết chồng chất đưa ra một quan điểm kỳ lạ cho rằng bằng cách nào đó phôtôn đi qua cả hai khe cùng lúc rồi sau đó nó tự ảnh hưởng đến chính mình và tạo nên hình ảnh các vân như quan sát được trên màn ảnh. Song làm sao cùng một lúc một phôtôn lại có thể đi qua được cả hai khe?

Những người theo thuyết chồng chất lý luận như sau. Nếu chúng ta không biết một hạt làm gì, nó được phép làm đồng thời mọi thứ khả dĩ. Trong trường hợp của phôtôn, do không biết nó đi qua khe bên trái hay khe bên phải, nên chúng ta cứ giả sử rằng nó đi qua đồng thời cả hai khe. Mỗi khả năng được gọi là một *trạng thái*, và vì phôtôn thực hiện đồng thời cả hai khả năng nên nó được xem là một *trạng thái chồng chất*. Chúng ta biết rằng một phôtôn rời khỏi sợi dây tóc bóng đèn và chúng ta cũng biết rằng một phôtôn đập vào màn ảnh ở phía sau hai khe, song trong khoảng giữa, bằng cách nào đó nó tách ra thành hai "phôtôn ma" đi qua cả hai khe. Thuyết chồng chất có vẻ như khá ngớ ngẩn, song ít nhất nó cũng giải thích được hình ảnh các vân tạo thành

trong thí nghiệm Young được thực hiện với từng phôtôn riêng lẻ. Để so sánh, quan điểm cổ điển kiểu cũ cho rằng phôtôn chỉ đi qua một trong hai khe và chúng ta chỉ đơn giản không biết cụ thể là khe nào mà thôi - điều này có vẻ như dễ hiểu hơn nhiều so với quan điểm lượng tử, song không may nó lại không giải thích được kết quả quan sát.

Erwin Schrodinger, người đoạt giải Nobel về vật lý năm 1933, đã đặt ra một truyện ngụ ngôn có tên là "con mèo của Schrodinger", thường được sử dụng để giải thích khái niệm về sự chồng chất trạng thái. Hãy tưởng tượng một con mèo trong một cái hộp. Có hai khả năng về trạng thái của con mèo, đó là chết hoặc sống. Ban đầu chúng ta biết rằng con mèo nhất định phải ở một trạng thái cụ thể, vì chúng ta thấy nó còn sống. Lúc này, con mèo không ở trong một trạng thái chồng chất. Sau đó, chúng ta đặt một lọ chất độc xianua vào bên trong hộp cùng với con mèo và đóng nắp hộp lại. Chúng ta giờ lâm vào tình trạng không biết gì nữa vì chúng ta không thấy cũng không đo đạc được trạng thái của con mèo. Nó vẫn còn sống hay là nó đã giẫm lên lọ xianua và chết? Chúng ta có thể nói theo cách truyền thống là nó hoặc đã chết hoặc còn sống, nhưng chúng ta không biết cụ thể là nó rơi vào trạng thái nào. Tuy nhiên, thuyết lượng tử cho rằng con mèo đang ở tình trạng chồng chất của hai trạng thái - nó vừa chết vừa sống, nghĩa là thỏa mãn mọi khả năng. Sự chồng chất xuất hiện chỉ khi chúng ta không còn nhìn thấy một vật và đó là cách mô tả vật khi nó ở trong tình thế nhập nhằng không rõ ràng. Khi, cuối cùng, mở hộp ra, chúng ta thấy con mèo đã chết hoặc còn sống. Hành động nhìn vào con mèo buộc nó phải ở một trạng thái cụ thể và lúc đó trạng thái chồng chất cũng biến mất.

Đối với các bạn đọc cảm thấy không thoải mái với sự chồng chất, còn có một phe lượng tử thứ hai, ủng hộ cho một cách diễn giải khác về thí nghiệm của Young. Không may là, quan điểm thứ hai này cũng kỳ quặc không kém. *Cách giải thích đa vũ trụ* tuyên bố rằng sau khi rời khỏi sợi tóc bóng đèn, phôtôn có hai lựa chọn - hoặc đi qua khe bên trái hoặc đi qua khe bên phải - tại thời điểm đó vũ trụ tách thành hai vũ trụ, trong một vũ trụ phôtôn đi qua khe bên trái, còn trong vũ trụ kia, phôtôn đi qua khe bên phải. Hai vũ trụ này bằng cách nào đó tương tác với nhau, tạo ra hình ảnh các vân giao thoa. Những người theo cách giải thích đa vũ trụ tin rằng cứ mỗi khi một vật có khả năng rơi vào một trong nhiều trạng thái tiềm năng, thì vũ trụ lại tách ra thành nhiều vũ trụ, vì vậy mà mỗi khả năng đều được thỏa mãn ở một vụ trụ khác nhau. Sự sinh sôi vũ trụ như vậy được gọi là *đa vũ trụ*.

Dù chúng ta có chấp nhận sự chồng chất hay cách giải thích đa vũ trụ, thì thuyết lượng tử vẫn là một khoa học khó hiểu. Tuy nhiên, nó đã chứng tỏ mình là một lý thuyết khoa học thực tiễn và thành công nhất từ trước đến nay. Ngoài khả năng giải thích được kết quả thí nghiệm của Young, thuyết lượng tử còn giải thích thành công nhiều hiện tượng khác. Chỉ thuyết lượng tử mới cho phép các nhà vật lý tính toán được những hậu quả của các phản ứng hạt nhân trong các nhà máy điện nguyên tử; chỉ thuyết lượng tử mới có thể giải thích được những điều kỳ lạ của ADN; chỉ thuyết lượng tử mới giải thích được mặt trời chiếu sáng như thế nào; và chỉ thuyết lượng tử mới có thể được sử dụng để thiết kế các đầu đọc laser để đọc các đĩa CD trong máy nghe nhạc của bạn. Vì vậy, dù muốn hay không, chúng ta vẫn đang sống trong một thế giới lượng tử.

Trong tất cả các hệ quả của lý thuyết lượng tử, thì hệ quả quan trọng nhất về mặt công nghệ chính là máy tính lượng tử. Cùng với việc phá hủy độ an toàn của tất cả các mật mã hiện đại, máy tính lượng tử còn mở ra một kỷ nguyên mới về sức mạnh máy tính. Một trong những nhà tiên phong trong lĩnh vực máy tính lượng tử là nhà vật lý người Anh, David Deutsche, người bắt đầu làm việc với khái niệm này vào năm 1984, khi ông tham dự một cuộc hội thảo về lý thuyết tính toán. Trong khi nghe một diễn giả tại hội thảo, Deutsch đã chợt phát hiện ra một điều mà trước đây không để ý tới. Trước đây người ta ngầm giả định rằng tất cả các máy tính đều thực sự vận hành theo các định luật của vật lý cổ điển, song Deutsch tin chắc rằng các máy tính phải tuân theo các định luật của vật lý lượng tử, vì các định luật lượng tử là cơ bản hơn.

David Deutsch

Các máy tính thông thường vận hành ở cấp độ tương đối vĩ mô, cấp độ mà ở đó, các định luật lượng tử và định luật cổ điển là hầu như không thể phân biệt được. Vì vậy sẽ không thành vấn đề khi các nhà khoa học nói chung suy nghĩ về các máy tính thông thường thông qua vật lý học cổ điển. Tuy nhiên, ở cấp độ vi mô, hai hệ thống quy

luật là hoàn toàn khác nhau, và ở cấp độ này chỉ các định luật của vật lý học lượng tử mới là chính xác. Ở cấp độ vi mô, các định luật lượng tử bộc lộ những điều kỳ quặc thực sự của chúng và một máy tính được tạo dựng để tận dụng những quy luật này sẽ hành xử theo một cách hoàn toàn khác. Sau cuộc hội thảo, Deutsch trở về nhà và bắt đầu viết lại lý thuyết về máy tính dưới ánh sáng của cơ học lượng tử. Trong một bài báo công bố năm 1985, ông đã mô tả hệ máy tính lượng tử của mình vận hành theo các định luật của vật lý học lượng tử. Đặc biệt là ông đã giải thích máy tính lượng tử của ông khác với một máy tính thông thường như thế nào.

Hãy tưởng tượng rằng bạn có hai phiên bản của một vấn đề. Để trả lời cả hai bằng máy tính thông thường, bạn sẽ phải đưa vào phiên bản thứ nhất và đợi câu trả lời, sau đó mới đưa vào phiên bản thứ hai và đợi trả lời. Nói cách khác, một máy tính thông thường chỉ có thể xử lý một vấn đề một lần và nếu có một số vấn đề thì nó phải xử lý chúng một cách lần lượt. Tuy nhiên, với một máy tính lượng tử, hai vấn đề có thể được tổ hợp lại thành một chồng chất của hai trạng thái và nhập đồng thời vào máy tính - tự máy tính sẽ đưa vào một chồng chất của hai trạng thái, mỗi trạng thái cho một vấn đề. Hoặc, theo cách diễn giải nhiều vũ trụ, thì máy sẽ đi vào hai vũ trụ khác nhau và trả lời mỗi phiên bản của một vấn đề trong mỗi vũ trụ khác nhau. Bất chấp cách giải thích là như thế nào, máy tính lượng tử có thể xử lý hai vấn đề cùng một lúc bằng việc tận dụng các định luật của vật lý học lượng tử.

Để có một ý niệm nào đó về sức mạnh của máy tính lượng tử, chúng ta có thể so sánh việc vận hành của nó với máy tính

truyền thống bằng cách xem điều gì sẽ xảy ra nếu mỗi máy được sử dụng để giải quyết một vấn đề cụ thể. Chẳng hạn, hai loại máy tính được dùng để giải quyết bài toán tìm một số mà bình phương và lập phương của nó chứa tất cả các chữ số từ 0 đến 9 một lần và chỉ một lần. Nếu chúng ta thử số 19, ta có $19^2 = 361$ và $19^3 = 6859$. Số 19 không phù hợp với yêu cầu vì bình phương và lập phương của nó chỉ chứa các chữ số 1, 3, 5, 6, 8, 9, tức là thiếu các số 0, 2, 4, 7 và số 6 bị lặp lại hai lần.

Để giải bài toán này với máy tính thường, người sử dụng sẽ phải chấp nhận thực hiện theo cách sau. Người thực hiện nạp số 1 vào và sau đó để máy tính kiểm tra. Khi máy tính hoàn tất việc tính toán cần thiết, nó sẽ thông báo là số đó có thỏa mãn tiêu chí đặt ra hay không. Số 1 không thỏa mãn, vì vậy, người sử dụng lại nạp vào số 2 và đợi máy tính tính ra một kết quả khác và cứ tiếp tục như vậy, cho đến khi cuối cùng con số thích hợp được tìm thấy. Kết quả là số 69, vì $69^2 = 4.761$ và $69^3 = 328.509$, và các số này thực sự chứa đủ mười chữ số, mỗi chữ số xuất hiện một lần và chỉ một lần. Trong thực tế, số 69 là số duy nhất thỏa mãn điều kiện này. Rõ ràng là quá trình này rất mất thời gian, vì máy tính thường chỉ kiểm tra được mỗi lần một số. Nếu máy tính phải mất 1 giây để kiểm tra một số thì nó phải mất 69 giây để tìm ra kết quả. Ngược lại, một máy tính lượng tử sẽ tìm ra đáp số chỉ trong 1 giây.

Người sử dụng bắt đầu bằng việc biểu thị các số theo một cách đặc biệt để tận dụng sức mạnh của máy tính lượng tử. Một cách để biểu diễn các con số là dưới dạng các hạt quay - nhiều hạt cơ bản vốn dĩ xoay tròn, chúng có thể quay theo hướng đông hoặc hướng tây, giống như quả bóng rổ quay trên đầu ngón tay. Khi

một hạt quay về phía đông, nó biểu diễn số **1**, và khi nó quay về hướng tây, nó biểu diễn số **0**. Vì vậy, một chuỗi các hạt quay biểu diễn một chuỗi các số **1** và **0** hay là một số nhị phân. Chẳng hạn, 7 hạt, quay hướng đông, đông, tây, đông, tây, tây, tây tương ứng, biểu diễn số nhị phân **1101000**, tương đương với số thập phân 104. Dựa trên sự quay của chúng, một tổ hợp của 7 hạt quay có thể biểu diễn một số bất kỳ từ 0 đến 127.

Với một máy tính thường, người sử dụng sẽ phải nạp vào từng chuỗi riêng lẻ, chẳng hạn như tây, tây, tây, tây, tây, tây, đông, biểu diễn số **0000001**, đây đơn giản là số thập phân 1. Người vận hành sau đó sẽ phải đợi máy tính kiểm tra xem số này có phù hợp với điều kiện ban đầu hay không. Sau đó người sử dụng sẽ nạp tiếp số **0000010**, là một chuỗi các hạt quay biểu diễn số 2 và cứ tiếp tục như vậy. Như trước, các số sẽ phải được nạp vào mỗi lần một số, mà chúng ta đã biết là rất tốn thời gian. Tuy nhiên, nếu làm việc với một máy tính lượng tử, người sử dụng sẽ có một cách nạp số khác nhanh hơn nhiều. Vì mỗi hạt là cơ bản nên nó tuân theo các định luật của vật lý học lượng tử. Vì vậy, khi một hạt không quan sát được thì nó có thể ở vào tình trạng chồng chất của các trạng thái, tức là nó quay đồng thời theo cả hai hướng, và vì vậy biểu thị cả số **0** và **1** cùng một lúc. Một cách khác, chúng ta có thể cho rằng các hạt đi vào hai vũ trụ khác nhau: trong một vũ trụ nó quay theo hướng đông và biểu thị cho số **1** trong khi ở vũ trụ kia, nó quay theo hướng tây và biểu thị cho số **0**.

Sự chồng chất đạt được bằng cách sau. Hãy tưởng tượng là chúng ta có thể quan sát được một trong các hạt và nó quay theo hướng tây. Để thay đổi chiều quay của nó, chúng ta sẽ phải cung cấp một xung năng lượng đủ mạnh để kích cho hạt đó quay theo

hướng đông. Nếu chúng ta cung cấp một xung yếu, thì khi chúng ta may mắn, hạt sẽ thay đổi chiều quay của nó, và khi chúng ta không may, hạt sẽ vẫn tiếp tục quay theo hướng tây. Cho đến đây, hạt đã được quan sát rõ ràng và chúng ta có thể theo dõi quá trình quay của nó. Tuy nhiên, nếu hạt đang quay theo hướng tây và được đặt vào trong hộp, ngoài tầm quan sát của chúng ta, và nó được cung cấp một xung năng lượng yếu, thì chúng ta không biết được chiều quay của nó có thay đổi hay không. Nghĩa là hạt ở tình trạng chồng chất của sự quay theo hướng đông và quay theo hướng tây, giống như con mèo ở tình trạng chồng chất của chết và sống. Bằng cách lấy bảy hạt quay theo hướng tây, đặt chúng vào trong hộp và cung cấp một xung năng lượng yếu cho mỗi hạt, thì cả bảy hạt sẽ đều ở tình trạng chồng chất.

Với cả bảy hạt ở tình trạng chồng chất, chúng sẽ biểu diễn được mọi tổ hợp khả dĩ của sự quay theo hướng đông và tây. Bảy hạt đồng thời biểu diễn 128 trạng thái, hay 128 số khác nhau. Người sử dụng nhập bảy hạt, trong khi chúng vẫn đang ở tình trạng chồng chất, vào máy tính lượng tử và nó sau đó sẽ thực hiện việc tính toán của mình như thể nó đang kiểm tra đồng thời tất cả 128 số. Sau 1 giây, máy tính đưa ra kết quả là số 69, thỏa mãn điều kiện yêu cầu. Người sử dụng lấy 128 phép tính làm giá của một phép tính.

Máy tính lượng tử thách thức sự hiểu biết thông thường. Bỏ qua chi tiết đã diễn ra trong 1 giây, máy tính lượng tử có thể được xem xét theo hai cách khác nhau, phụ thuộc vào cách giải thích nào của cơ học lượng tử mà bạn thích hơn. Một số nhà vật lý coi máy tính lượng tử như là một thực thể duy nhất thực hiện được sự tính toán đồng thời với 128 số. Quan điểm khác coi nó

là 128 thực thể, mỗi thực thể là một vũ trụ riêng biệt, mỗi thực thể thực hiện chỉ một phép tính. Tính toán lượng tử là công nghệ của *vùng tranh tối tranh sáng*.

Khi máy tính truyền thống thường vận hành trên các xâu gồm các số **1** và số **0**, các số **1** và các số **0** được gọi là các *bit*, viết tắt của *binary digit* (số nhị phân). Vì máy tính lượng tử xử lý các chuỗi số **1** và **0** ở tình trạng chồng chất lượng tử, nên chúng được gọi là bit lượng tử hay *qubit* (phát âm là *cubits)*. Lợi thế của qubit trở nên rõ ràng hơn khi chúng ta xem xét nhiều hạt hơn. Với 250 hạt quay, hay 250 qubit, nó có thể biểu thị cho 10^{75} tổ hợp, nhiều hơn số nguyên tử trong vũ trụ. Nếu có thể đạt được sự chồng chất thích hợp với 250 hạt, thì máy tính lượng tử có thể thực hiện đồng thời 10^{75} phép tính, chỉ trong vòng 1 giây.

Việc khai thác các hiệu ứng lượng tử có thể dẫn đến máy tính lượng tử với sức mạnh không thể tưởng tượng nổi. Không may là khi Deutsch sáng tạo ra hệ máy tính lượng tử của mình vào giữa những năm 1980, không một ai biết làm thế nào để chế tạo được một máy tính như thế trong thực tế. Chẳng hạn, các nhà khoa học không thể thực sự chế tạo ra bất cứ thứ gì có thể tính toán với các hạt quay ở tình trạng chồng chất trạng thái. Một trong những rào cản lớn nhất là vẫn duy trì sự chồng chất các trạng thái trong suốt quá trình tính toán. Một tình trạng chồng chất tồn tại chỉ khi nó không được quan sát, song quan sát theo nghĩa chung nhất bao gồm bất kỳ một sự tương tác nào với bất kỳ thứ gì ở bên ngoài đối với tình trạng chồng chất đó. Một nguyên tử riêng lẻ lang thang tương tác với một trong các hạt quay sẽ khiến cho sự chồng chất rơi vào một trạng thái và làm cho việc tính toán lượng tử hoàn toàn thất bại.

Một vấn đề khác là các nhà khoa học không tìm ra cách nào để lập trình cho một máy tính lượng tử, và vì vậy không biết chắc chắn nó có thể thực hiện những loại tính toán nào. Tuy nhiên, vào năm 1994, Peter Shor của Phòng Thí nghiệm AT&T Bell ở New Jersey đã thành công trong việc xác định một chương trình hữu dụng cho máy tính lượng tử. Một tin tức quan trọng đối với các nhà giải mã đó là chương trình của Shor đã vạch ra một chuỗi các bước mà một máy tính lượng tử cần thực hiện để phân tích một số cực lớn ra thừa số - đó chính là điều cần thiết để hóa giải mật mã RSA. Khi Martin Gardner đưa ra câu đố về RSA trên tờ *Scientific American*, 600 máy tính đã phải làm việc cật lực trong vài tháng mới phân tích được một số gồm 129 chữ số ra thừa số nguyên tố. Để so sánh, chương trình của Shor có thể phân tích ra thừa số một số lớn hơn một triệu lần, nhưng trong thời gian chỉ bằng 1 phần triệu. Không may là Shor không thể thực thi chương trình phân tích ra thừa số của mình, vì vẫn chưa có máy tính lượng tử.

Sau đó, vào năm 1996, Lov Grover, cũng tại Phòng thí nghiệm Bell, đã khám phá ra một chương trình rất mạnh khác. Chương trình của Grover là một cách tìm kiếm một danh sách với tốc độ cực cao, nó xem ra không có gì thú vị đặc biệt nếu bạn không biết rằng đó chính xác là điều cần có để giải mật mã DES. Để phá vỡ một mật mã DES thì cần tìm kiếm một danh sách tất cả các chìa khóa mã tiềm năng để tìm ra chìa khóa mã đúng. Nếu một máy tính thông thường có thể kiểm tra một triệu chìa khóa mã trong một giây thì nó phải mất 1.000 năm để phá vỡ nổi mật mã DES, trong khi một máy tính lượng tử sử dụng chương trình của Grover có thể tìm thấy chìa khóa mã trong vòng chưa đến 4 phút.

Hoàn toàn tình cờ khi hai chương trình máy tính lượng tử đầu tiên được phát minh lại chính là điều mà các nhà giải mã hiện đặt lên hàng đầu danh sách những điều mơ ước của họ. Mặc dù chương trình của Shor và Grover đã tạo nên niềm lạc quan vô cùng to lớn trong các nhà giải mã, song vẫn còn sự thất vọng lớn vì vẫn chưa có một máy tính lượng tử thực sự để có thể chạy được các chương trình này. Không có gì ngạc nhiên khi mà tiềm năng của thứ vũ khí tối thượng trong công nghệ giải mã lại gợi sự thèm muốn của các tổ chức như Cơ quan các Dự án Nghiên cứu Quốc phòng Tiên tiến (DARPA) và Phòng thí nghiệm quốc gia Los Alamos, những tổ chức đang cố gắng một cách độc lập nhằm chế tạo được những thiết bị có thể xử lý các qubit tương tự như chíp silicon xử lý các bit. Mặc dù một số thành quả gần đây đã khích lệ tinh thần các nhà nghiên cứu rất nhiều, song công bằng mà nói thì công nghệ vẫn còn rất sơ khai. Năm 1998, Serge Haroche của trường Đại học Paris VI đã đặt những điều phóng đại, cường điệu xung quanh những thành quả đó vào đúng vị trí khi ông bác bỏ những tuyên bố cho rằng máy tính lượng tử thực sự sẽ đạt được trong vài năm tới. Ông nói điều này chẳng khác gì việc cần mẫn lắp ráp lớp thứ nhất của một ngôi nhà bằng những quân bài rồi sau đó khuếch khoác rằng lắp tiếp 15.000 lớp nữa chỉ đơn giản là vấn đề thủ tục.

Chỉ có thời gian mới trả lời được là liệu các vấn đề chế tạo một máy tính lượng tử có thể vượt qua được hay không và nếu được thì khi nào. Vì vậy trong khi chờ đợi, chúng ta chỉ có thể suy luận về những ảnh hưởng của nó đối với thế giới của khoa học mật mã. Kể từ những năm 1970, các nhà tạo mã rõ ràng đã vượt lên trong cuộc đua với các nhà giải mã, nhờ những mật mã

như DES và RSA. Các loại mật mã này đúng là một nguồn quý báu, vì chúng hoàn toàn đáng tin cậy để mã hóa thư điện tử và bảo vệ bí mật riêng tư của chúng ta. Tương tự, khi bước vào thế kỷ 21, ngày càng nhiều hoạt động thương mại được thực hiện trên Internet, và thị trường điện tử sẽ phải dựa vào các mật mã mạnh để bảo vệ và xác nhận các giao dịch tài chính. Khi thông tin trở thành hàng hóa có giá trị nhất trên thế giới, vận mệnh về kinh tế, chính trị và quân sự của các quốc gia sẽ phụ thuộc vào sức mạnh của mật mã.

Do vậy, việc phát triển một máy tính lượng tử vận hành một cách đầy đủ sẽ gây nguy hiểm cho bí mật cá nhân, làm phương hại đến thương mại điện tử và phá hỏng khái niệm an ninh quốc gia. Một máy tính lượng tử sẽ hủy hoại sự ổn định của thế giới. Quốc gia nào đạt đến đó trước tiên sẽ có khả năng kiểm soát được thông tin liên lạc của mọi công dân nước mình, đọc được ý nghĩ của mọi đối thủ về thương mại và nghe được mọi kế hoạch của kẻ thù. Mặc dù vẫn còn đang trong giai đoạn phôi thai, song tính toán lượng tử đang đặt ra mối đe dọa tiềm tàng đối với cá nhân, với kinh doanh quốc tế và với an ninh toàn cầu.

Mật mã lượng tử

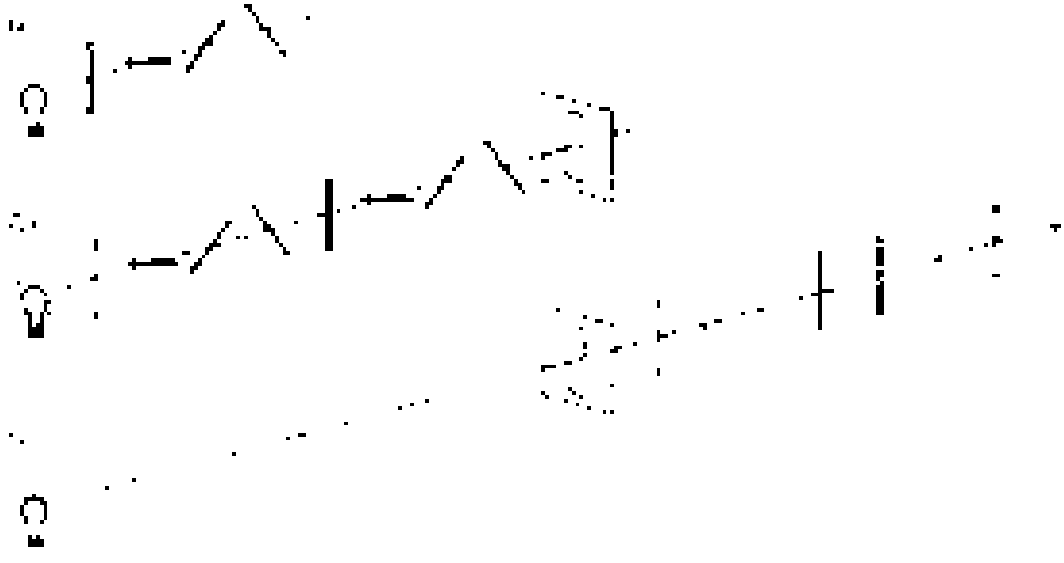
Trong khi các nhà giải mã đang tiên liệu sự ra đời của các máy tính lượng tử, thì các nhà tạo mã vẫn đang tìm kiếm điều thần kỳ về công nghệ của mình - tức là một hệ thống mã hóa có khả năng tái thiết sự bí mật riêng tư ngay cả khi phải đương đầu với sức mạnh của một máy tính lượng tử. Hình thái mã hóa mới này khác biệt về cơ bản với bất kỳ dạng mã hóa nào mà chúng ta gặp

trước đây ở chỗ nó mang lại niềm hy vọng cho sự bí mật tuyệt đối. Nói cách khác, hệ thống này không có sơ hở và sẽ bảo đảm một độ an toàn tuyệt đối vĩnh viễn. Hơn nữa, nó cũng lại dựa trên lý thuyết lượng tử, cơ sở của máy tính lượng tử. Do vậy trong khi lý thuyết lượng tử chính là nguồn cảm hứng của loại máy tính có thể phá vỡ mọi loại mật mã thì nó cũng chính là trái tim của một mật mã mới không thể phá vỡ nổi được gọi là *mật mã lượng tử.*

Câu chuyện về mật mã lượng tử bắt đầu từ một ý tưởng kỳ lạ được đưa ra vào cuối những năm 1960 bởi Stephen Wiesner, lúc đó là nghiên cứu sinh tại Đại học Columbia. Thật đáng buồn là Wiesner đã không may phát minh ra một ý tưởng đi trước thời đại đến mức chẳng ai ngó ngàng đến một cách nghiêm túc. Ông vẫn còn nhớ phản ứng của những người đi trước: "Tôi không nhận được sự ủng hộ nào từ người hướng dẫn luận án - ông ấy hoàn toàn không để ý gì đến nó hết. Tôi cũng trình bày với một số người khác, nhưng tất cả họ đều có vẻ mặt lạ lùng, rồi quay trở lại với công việc mà họ đang làm". Wiesner đã đưa ra khái niệm kỳ quặc là tiền lượng tử, với lợi ích rất lớn, đó là ngăn chặn được nạn tiền giả.

Tiền lượng tử của Wiesner chủ yếu dựa trên vật lý về phôtôn. Khi một phôtôn chuyển động qua không gian, nó dao động, như minh họa trên Hình 73 (a). Cả bốn phôtôn đều chuyển động theo cùng một hướng, song góc dao động trong bốn trường hợp là khác nhau. Góc dao động được gọi là phân cực của phôtôn và bóng đèn tạo ra các phôtôn với đủ loại phân cực, tức là một số phôtôn dao động lên xuống, một số từ bên này qua bên kia, số khác theo mọi góc trung gian. Để đơn giản hóa vấn đề, chúng ta giả sử rằng các phôtôn có bốn phân cực khả dĩ được ký hiệu là [illegible].

Bằng cách đặt một tấm lọc gọi là Polaroid (kính phân cực) trên đường đi của phôtôn, ta có thể chắc chắn rằng tia sáng ló ra sau Polaroid có chứa các phôtôn dao động chỉ theo một hướng nhất định; nói cách khác, tất cả các phôtôn này đều có cùng phân cực. Trên một phương diện nào đó, chúng ta có thể coi Polaroid như là một lưới sắt và các phôtôn như là các que diêm được ném một cách ngẫu nhiên vào lưới sắt đó. Các que diêm sẽ chỉ lọt qua lưới sắt khi chúng tới dưới một góc đúng. Bất kỳ phôtôn nào phân cực cùng hướng với tấm Polaroid sẽ tự động đi qua nó mà không thay đổi, còn những phôtôn nào phân cực vuông góc với tấm lọc sẽ bị chặn lại.



Hình 73 (a) Mặc dù các phôtôn ánh sáng dao động theo mọi hướng, song để đơn giản hóa, chúng ta giả định chỉ có bốn hướng khác nhau như trong hình. (b) Đèn phát ra 8 phôtôn, dao động theo các hướng khác nhau. Mỗi phôtôn có một phân cực. Các phôtôn hướng về phía tấm Polaroid thẳng đứng. (c) Ở phía bên kia của tấm lọc, chỉ có một nửa số phôtôn sống sót. Các phôtôn phân cực thẳng đứng đi qua, và các phôtôn phân cực ngang bị chặn lại. Một nửa số phôtôn phân cực chéo cũng đi qua và vì vậy chúng đổi hướng phân cực thành thẳng đứng.

Không may là sự tương tự với que diêm không còn nữa khi ta xét đến các phôtôn phân cực chéo khi tiến đến gần một tấm Polaroid thẳng đứng. Mặc dù các que diêm có hướng chéo sẽ bị chặn lại bởi một lưới sắt thẳng đứng, song lại thực sự không đúng với các phôtôn phân cực chéo tiến đến một tấm Polaroid thẳng đứng. Thực tế, các phôtôn phân cực chéo ở trong một tình huống nhoè lượng tử khi phía trước là tấm Polaroid thẳng đứng. Điều thực sự xảy ra là một nửa trong số chúng bị chặn lại một cách ngẫu nhiên, và nửa còn lại thì đi qua, và số đi qua đó sẽ đổi hướng dao động theo chiều thẳng đứng. Hình 73(b) cho thấy tám phôtôn tiến đến một tấm Polaroid thẳng đứng, còn Hình 73(c) cho thấy chỉ có 4 phôtôn lọt qua. Tất cả các phôtôn phân cực thẳng đứng đều đi qua, tất cả các phôtôn phân cực ngang bị chặn lại và một nửa số phôtôn phân cực chéo lọt qua.

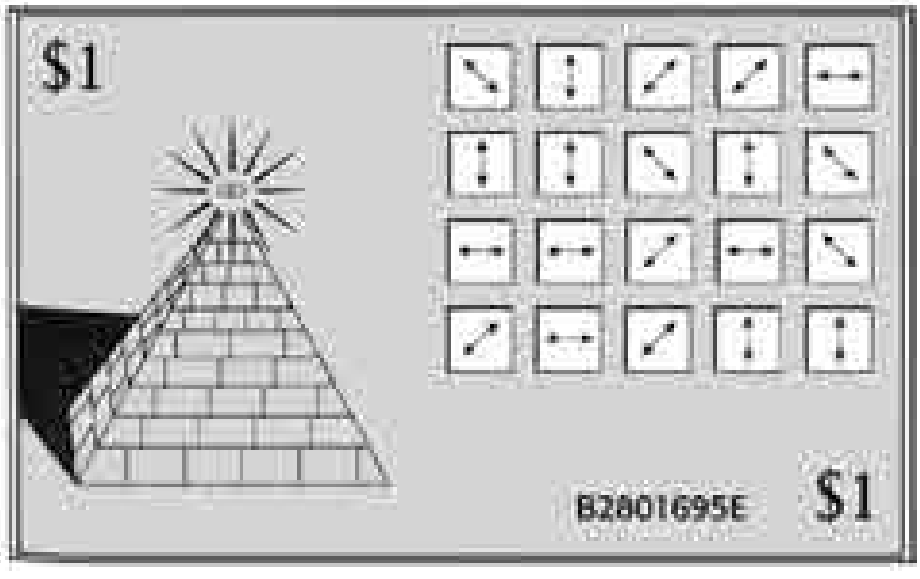
Chính khả năng chặn lại một số phôtôn nhất định này đã giải thích sự hoạt động của các kính râm Polaroid. Thực tế, bạn có thể chứng minh tác dụng của tấm lọc Polaroid bằng cách thí nghiệm với một cặp kính râm này. Trước hết, hãy tháo ra một mắt kính và nhắm mắt này lại để bạn chỉ nhìn bằng mắt kia qua mắt kính còn lại. Không có gì ngạc nhiên là xung quanh trông tối sầm lại vì mắt kính chặn lại rất nhiều phôtôn lẽ ra phải đi vào mắt bạn. Lúc này, tất cả các phôtôn đi vào mắt bạn đều có cùng phân cực. Sau đó, lấy mắt kính đã tháo ra đặt phía trước mắt kính bạn đang đeo rồi xoay từ từ. Tại một vị trí trong quá trình quay này, mắt kính di động không ảnh hưởng tới lượng ánh sáng đi vào mắt bạn vì sự định hướng của nó trùng với sự định hướng của mắt kính cố định - tất cả các phôtôn đi qua mắt kính di động cũng sẽ đi qua mắt kính cố định. Nếu giờ bạn quay mắt kính di động

đi 90^0, tất cả sẽ biến thành màu đen. Ở vị trí này, sự phân cực của mắt kính di động vuông góc với phân cực của mắt kính cố định, nên bất kỳ phôtôn nào qua được mắt kính di động đều bị chặn lại bởi mắt kính cố định. Nếu bạn quay 45^0, bạn sẽ đạt đến trạng thái trung gian, trong đó các mắt kính phần nào đó không thẳng hàng với nhau và một nửa phôtôn đi qua mắt kính di động sẽ đi qua mắt kính cố định.

Wiesner đã dự định sử dụng sự phân cực của các phôtôn để chế tạo những tờ giấy bạc đôla không bao giờ bị làm giả. Ý tưởng của ông là các tờ giấy bạc đôla sẽ chứa trong nó 20 bẫy ánh sáng, tức là những thiết bị bé xíu có khả năng bắt và giữ lại các phôtôn. Ông khuyến nghị các ngân hàng sử dụng bốn tấm lọc Polaroid với bốn định hướng khác nhau để chứa 20 bẫy ánh sáng với một chuỗi 20 phôtôn phân cực, mỗi đồng giấy bạc sử dụng một chuỗi khác nhau.

Ví dụ, trên Hình 74 là một tờ giấy bạc 1 đôla với chuỗi phân cực . Mặc dù các phân cực được thể hiện tường minh trong Hình 74, song trên thực tế ta không thể nhìn thấy chúng bằng mắt thường. Mỗi tờ giấy bạc cũng vẫn có số sêri như thường lệ, là B2801695E đối với tờ 1 đôla trong hình. Ngân hàng phát hành có thể xác nhận đồng đôla theo chuỗi phân cực và số sêri của nó, và giữ danh sách gốc toàn bộ số sêri và chuỗi phân cực tương ứng.

Một kẻ làm tiền giả giờ đây phải đối mặt với một vấn đề - đó là hắn không đơn giản làm giả đồng đôla với số sêri tùy ý và chuỗi phân cực ngẫu nhiên trong các bẫy ánh sáng, vì cặp đặc tính này sẽ không có trong danh sách gốc của ngân hàng và ngân hàng sẽ phát hiện ra ngay đồng đôla đó là giả. Để việc làm giả có hiệu



Hình 74 Tiền lượng tử của Stephen Wiesner. Mỗi tờ bạc là duy nhất vì số sêri của nó, có thể nhìn thấy dễ dàng, và 20 bẫy ánh sáng, có nội dung hoàn toàn bí mật. Bẫy ánh sáng có chứa các phôtôn phân cực khác nhau. Ngân hàng biết chuỗi các phân cực tương ứng với số sêri, song kẻ làm tiền giả thì không biết.

quả, kẻ làm tiền giả phải sử dụng một tờ tiền thật để làm mẫu, bằng cách nào đó tính toán được 20 phân cực của nó rồi sau đó làm một đồng đôla y hệt, sao chép toàn bộ số sêri và đặt các bẫy ánh sáng một cách phù hợp. Tuy nhiên, việc đo các phân cực của phôtôn là một nhiệm vụ cực kỳ tinh xảo, và nếu kẻ làm giả không đo được một cách chính xác thì hắn không thể hy vọng làm được một tờ y hệt như thật.

Để hiểu được việc đo phân cực của các phôtôn khó khăn như thế nào, chúng ta cần xét xem sẽ phải xoay xở như thế nào để thực hiện một phép đo như vậy. Chỉ có một cách duy nhất để biết được điều gì đó về phân cực của các phôtôn, đó là sử dụng một tấm lọc Polaroid. Để đo phân cực của phôtôn trong một bẫy ánh sáng nhất định, kẻ làm giả lựa chọn một tấm Polaroid và định hướng nó theo một phương nhất định, chẳng hạn như thẳng đứng, ↕.

Nếu phôtôn đi ra từ bẫy ánh sáng cũng phân cực thẳng đứng thì nó sẽ đi qua tấm Polaroid và kẻ làm giả giả định một cách chính xác rằng nó là một phôtôn phân cực thẳng đứng. Nếu phôtôn đi ra có phân cực nằm ngang thì nó sẽ không qua tấm polaroid thẳng đứng và kẻ làm tiền giả biết được phôtôn đó phân cực ngang. Tuy nhiên, nếu phôtôn đi ra phân cực chéo (↘ hay ↗), nó có thể hoặc không thể đi qua tấm lọc, và dù là trường hợp nào thì kẻ làm tiền giả cũng không thể xác định được bản chất thật của nó. Một phôtôn ↘ có thể đi qua tấm lọc Polaroid thẳng đứng, trong trường hợp đó kẻ làm giả lại giả định sai rằng đó là một phôtôn phân cực thẳng đứng, hoặc cũng phôtôn đó nhưng không đi qua tấm lọc, thì hắn lại tưởng nhầm đấy là phôtôn phân cực ngang. Có một cách khác, nếu kẻ làm giả lựa chọn đo phôtôn trong một bẫy ánh sáng khác bằng cách đặt tấm lọc nằm chéo, chẳng hạn ↘, thì có thể xác định đúng các phôtôn phân cực chéo, song lại sai khi xác định các phôtôn phân cực ngang hoặc thẳng đứng.

Vấn đề của kẻ làm tiền giả là hắn phải sử dụng sự định hướng đúng của tấm lọc Polaroid để xác định phân cực của các phôtôn, song lại không biết hướng nào là đúng vì hắn không biết phân cực của các phôtôn. Tình huống catch-22 (xem giải thích ở Chương 7) này là một bộ phận cố hữu của vật lý học phôtôn. Hãy tưởng tượng rằng kẻ làm giả tiền lựa chọn sự định hướng tấm lọc là ↘ để đo phôtôn đi ra từ bẫy ánh sáng thứ hai, và phôtôn không đi qua tấm lọc. Từ đó hắn biết chắc rằng phân cực của phôtôn đó không phải là ↘ vì phôtôn có phân cực này nhất thiết sẽ phải đi qua. Tuy nhiên, hắn lại không thể biết chắc phôtôn đó có phân cực loại ↗ hay không vì các phôtôn có phân cực ↕ hoặc ↔ cũng đều có xác suất 50% bị chặn lại.

Sự khó khăn trong việc đo phôtôn là một khía cạnh của nguyên lý bất định, được nhà vật lý Đức Werner Heisenberg đưa ra vào những năm 1920. Ông đã dịch một mệnh đề có tính kỹ thuật cao thành một phát biểu đơn giản như sau: "Về nguyên tắc, chúng ta *không thể* biết hiện tại với đầy đủ mọi chi tiết của nó". Điều này không có nghĩa là chúng ta không thể biết mọi thứ vì chúng ta không có đủ thiết bị đo hay vì thiết bị của chúng ta được thiết kế tồi. Mà theo Heisenberg, thì về mặt logic, không thể đo được mọi khía cạnh của một vật cụ thể một cách tuyệt đối chính xác. Trong trường hợp cụ thể đang xét, chúng ta không thể đo được mọi khía cạnh của các phôtôn trong các bẫy ánh sáng một cách tuyệt đối chính xác. Nguyên lý bất định là một hệ quả kỳ quặc khác của lý thuyết lượng tử.

Tiền lượng tử của Wiesner dựa trên thực tế việc làm giả là một quá trình gồm hai bước: thứ nhất là kẻ làm giả cần phải đo đạc tờ giấy bạc mẫu một cách chính xác, và sau đó hắn phải sao chép giống y hệt. Bằng việc đưa các phôtôn vào thiết kế của đồng bạc đôla, Wiesner làm cho đồng tiền không thể đo đạc được một cách chính xác và vì vậy tạo nên một rào cản đối với việc làm giả.

Một kẻ làm tiền giả ngây thơ có thể nghĩ rằng nếu mình không thể đo được phân cực của các phôtôn trong các bẫy ánh sáng thì ngân hàng cũng không thể. Hắn có thể thử sản xuất các đồng đôla bằng cách cho vào các bẫy ánh sáng một chuỗi các phân cực tùy ý. Tuy nhiên, ngân hàng vẫn có thể xác định được đồng đôla nào là thật. Ngân hàng nhìn vào số sêri, sau đó tra cứu danh sách mật của mình để xem phôtôn nào trong mỗi bẫy ánh sáng. Vì ngân hàng đã biết trước phân cực nào ở trong mỗi bẫy ánh sáng nên nó có thể đặt đúng hướng tấm Polaroid để thực hiện phép

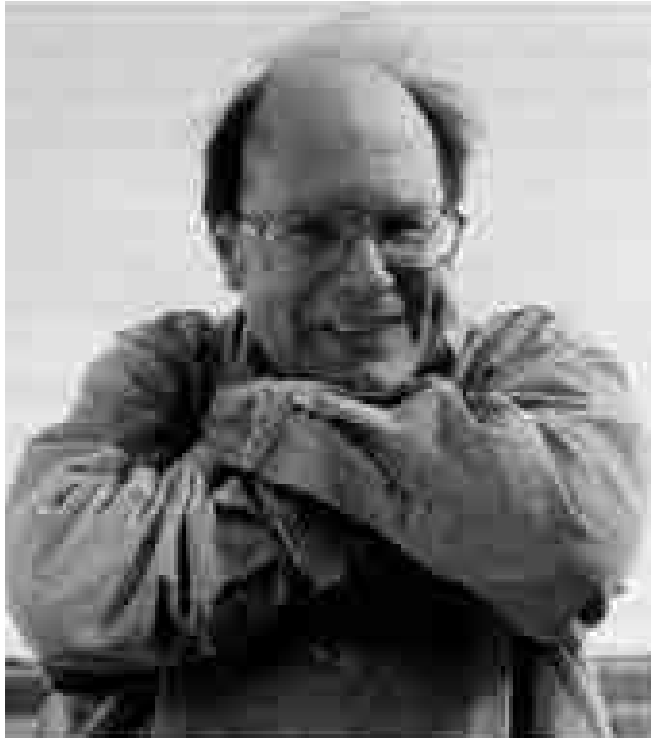
đo một cách chính xác. Nếu tờ giấy bạc là giả, các phân cực tùy tiện của kẻ làm giả sẽ dẫn đến phép đo không đúng và tờ bạc giả sẽ bị loại ra. Chẳng hạn, nếu ngân hàng sử dụng một tấm lọc có định hướng ⁝ để đo phôtôn có hướng dao động ⁝, song lại thấy tấm lọc chặn phôtôn lại, chứng tỏ kẻ làm giả đã đặt sai phôtôn vào bẫy. Tuy nhiên, nếu tờ giấy bạc hóa ra là thật thì ngân hàng sẽ đặt lại vào các bẫy ánh sáng các phôtôn thích hợp rồi đưa trở lại lưu thông.

Tóm lại, một kẻ làm tiền giả không thể đo được phân cực trong một tờ bạc thật vì hắn không biết loại phôtôn nào trong mỗi bẫy ánh sáng và vì vậy không thể biết hướng đặt tấm Polaroid để đo đạc nó một cách chính xác. Trái lại, ngân hàng có thể kiểm tra các phân cực trong một tờ bạc thật vì ban đầu chính họ đã lựa chọn phân cực và vì vậy biết đặt hướng tấm Polaroid như thế nào.

Tiền lượng tử là một ý tưởng tuyệt vời. Nhưng nó cũng hoàn toàn phi thực tế. Điểm đầu tiên là các kỹ sư vẫn chưa phát minh ra công nghệ để giữ các phôtôn ở một trạng thái phân cực nhất định trong một thời gian dài. Ngay cả nếu công nghệ đó thực sự tồn tại đi nữa thì cũng sẽ rất tốn kém để thực hiện được điều đó. Có thể sẽ phải chi 1 triệu đôla để bảo vệ cho đồng bạc 1 đôla. Mặc dù là phi thực tế song tiền lượng tử đã vận dụng lý thuyết lượng tử theo một cách rất hấp dẫn và giàu trí tưởng tượng nên dù không được sự ủng hộ của người hướng dẫn, Wiesner vẫn gửi một bài báo tới một tạp chí khoa học. Nhưng nó đã bị từ chối. Ông gửi tiếp cho ba tạp chí khác và cả ba lần cũng đều bị từ chối. Wiesner phàn nàn rằng họ đơn giản là không hiểu gì về vật lý cả.

Dường như là chỉ có một người chia sẻ niềm hứng khởi về khái niệm tiền lượng tử với Wiesner. Đó là một người bạn cũ tên là Charles Bennett, vài năm trước đã cùng là sinh viên với Wiesner ở Đại học Brandeis. Sự ham hiểu biết của Bennett về mọi khía cạnh của khoa học là điều đáng nói nhất về tính cách của anh. Anh nói rằng từ lúc mới ba tuổi anh đã muốn là một nhà khoa học, và sự say mê thời niên thiếu của anh đối với lĩnh vực này đã không bị suy giảm là nhờ mẹ của anh. Một hôm về nhà, bà thấy một cái nồi có chứa một món hầm kỳ quặc đang sôi sùng sục trên bếp. May mắn là bà đã không nếm thử vì hóa ra nó là phần còn lại của một con rùa đã bị cậu bé Bennett nấu với kiềm để lọc thịt ra khỏi xương, nhờ đó đã thu được một một mẫu khung xương rùa hoàn hảo. Trong thời niên thiếu, sự ham hiểu biết của Bennett đã chuyển từ sinh học sang hóa sinh học, và khi tới Brandeis, anh đã quyết định theo chuyên ngành hóa học. Ở trường sau đại học, anh tập trung vào hóa lý, sau đó chuyển sang nghiên cứu vật lý, toán học, logic và cuối cùng là khoa học máy tính.

Biết được mối quan tâm rộng lớn của Bennett, Wiesner hy vọng là anh sẽ hiểu rõ giá trị của tiền lượng tử, nên đã đưa cho anh tập bản thảo đã bị các báo từ chối. Bennett ngay lập tức thấy khái niệm này rất hấp dẫn và xem đó là một trong những ý tưởng tuyệt vời nhất mà anh từng gặp. Trong hơn một thập kỷ sau đó, anh thường đọc lại bản thảo này, và luôn tự hỏi liệu có cách nào biến ý tưởng tài tình như vậy thành một cái gì đó hữu dụng hay không. Ngay cả khi đã là một cán bộ nghiên cứu tại Phòng thí nghiệm Thomas J. Watson của IBM vào đầu những năm 1980, Bennett vẫn không ngừng suy ngẫm về ý tưởng của Wiesner. Các tạp chí có thể không muốn đăng nó song Bennett thì lại bị nó ám ảnh.



Charles Bennett

Một hôm, Bennett giải thích khái niệm về tiền lượng tử cho Gilles Brassard, một nhà khoa học về máy tính ở Đại học Montreal. Bennett và Brassard vốn đã từng cộng tác trong nhiều dự án nghiên cứu, họ đã thảo luận nhiều lần về những phức tạp trong bài báo của Wiesner. Dần dần họ bắt đầu nhận thấy ý tưởng của Wiesner có thể ứng dụng được trong khoa học mật mã. Đối với Eve, để giải mã một bức thư đã được mã hóa giữa Bob và Alice, trước tiên cô ta phải chặn bắt được nó, tức là bằng cách nào đó phải nắm được chính xác nội dung được truyền đi. Tiền lượng tử của Wiesner là an toàn vì không thể nắm bắt được một cách chính xác phân cực của các phôtôn bị giữ lại trên đồng bạc. Bennett và Brassard đã băn khoăn tự hỏi điều gì sẽ xảy ra nếu một bức thư đã mã hóa được biểu diễn và truyền đi bằng một chuỗi các phôtôn phân cực. Về lý thuyết, dường như Eve sẽ không thể đọc được một cách chính xác bức thư mã hóa, và nếu đã không thể đọc được thư thì cũng không thể giải mã được nó.

Bennett và Brassard bắt đầu thiết lập một hệ thống dựa trên nguyên lý như sau. Hãy tưởng tượng rằng Alice muốn gửi cho Bob một bức thư mã hóa, có chứa một xâu các số **1** và các số **0**. Cô biểu diễn các số **1** và **0** bằng cách gửi đi các phôtôn có phân

cực nhất định. Alice có hai sơ đồ khả thi để gán phân cực của các phôtôn cho các số **1** và **0**. Trong sơ đồ thứ nhất, được gọi là *thẳng* hay sơ đồ +, cô gửi để biểu diễn số **1**, và để biểu diễn số **0**. Trong sơ đồ thứ hai, gọi là *chéo* hay sơ đồ ×, cô gửi để biểu diễn số **1** và để biểu diễn số **0**. Để gửi một bức thư nhị phân, cô sẽ hoán đổi giữa hai sơ đồ trên với nhau theo một cách không thể dự đoán trước được. Vì vậy, bức thư nhị phân **1101101001** có thể được chuyển đi như sau:

Bức thư	**1 1 0 1 1 0 1 0 0 1**
Sơ đồ	+ × + × × × + + × ×
Truyền đi	

Alice sử dụng sơ đồ + để truyền đi số **1** thứ nhất, và sơ đồ × để truyền đi số **1** thứ hai. Như vậy, ở cả hai trường hợp đều truyền đi cùng số **1**, song mỗi lần được biểu diễn bằng các phôtôn có phân cực khác nhau.

Nếu Eve muốn bắt được bức thư này, cô ta cần phải nhận dạng được phân cực của mỗi phôtôn, cũng giống như kẻ làm tiền giả phải nhận dạng được phân cực của phôtôn trong các bẫy ánh sáng của đồng đôla. Để đo được phân cực của mỗi phôtôn, Eve phải quyết định hướng đặt tấm Polaroid của mình như thế nào mỗi khi có một phôtôn đi tới. Cô ta không thể biết chắc Alice sử dụng sơ đồ nào cho mỗi phôtôn, nên đành chọn bừa và sai đến một nửa. Do vậy, cô không thể hiểu được đầy đủ cách truyền đi của Alice.

Một cách khác để suy xét dễ dàng hơn tình trạng lưỡng nan của Eve đó là giả sử rằng cô có hai kiểu máy dò Polaroid để tùy ý sử dụng. Máy dò + có thể đo được các phôtôn phân cực ngang và thẳng đứng với độ chính xác hoàn hảo song lại không thể đo

được chính xác các phôtôn phân cực chéo, và dễ hiểu sai rằng chúng là các phôtôn phân cực ngang hoặc thẳng đứng. Mặt khác, máy dò × có thể đo được các phôtôn phân cực chéo với độ chính xác hoàn hảo song lại không thể đo các phôtôn phân cực ngang và thẳng đứng một cách chắc chắn và dễ hiểu sai chúng là các phôtôn phân cực chéo. Chẳng hạn, nếu Eve sử dụng máy dò × để đo phôtôn đầu tiên, là , cô sẽ hiểu nhầm rằng nó là hoặc . Nếu cô hiểu nhầm rằng nó là , thì không có vấn đề gì vì nó cũng biểu diễn số **1**, song nếu cô dịch nhầm ra là thì sẽ gặp rắc rối vì nó biểu diễn số **0**. Vấn đề còn tồi tệ hơn đối với Eve, vì cô chỉ có một cơ hội để đo phôtôn một cách chính xác. Một phôtôn là không thể chia nhỏ được nên cô không thể chia nó thành hai phôtôn và sử dụng cả hai sơ đồ để đo.

Hệ thống này có một số đặc tính thú vị. Eve không thể chắc chắn chặn bắt được chính xác bức thư được mã hóa nên cô không có hy vọng giải mã được nó. Tuy nhiên, hệ thống lại có một vấn đề nghiêm trọng và rõ ràng là không thể khắc phục được - đó là Bob cũng ở cùng vị thế như Eve, bởi vì anh không có cách nào biết được Alice sử dụng sơ đồ phân cực nào cho mỗi phôtôn, nên anh cũng sẽ giải thích sai bức thư. Giải pháp rõ ràng cho vấn đề này đối với Alice và Bob là họ phải thỏa thuận sẽ dùng sơ đồ phân cực nào cho mỗi phôtôn. Đối với ví dụ trên, Alice và Bob sẽ phải cùng chia sẻ một danh sách, hay chìa khóa, cụ thể là + × + × × × + + × ×. Tuy nhiên, đến đây chúng ta lại trở về vấn đề phân phối chìa khóa mã, cụ thể là bằng cách nào đó Alice phải gửi danh sách các sơ đồ phân cực cho Bob một cách an toàn.

Tất nhiên, Alice có thể mã hóa danh sách các sơ đồ này bằng cách sử dụng mật mã chìa khóa công khai như RSA, và sau đó

chuyển đến Bob. Tuy nhiên, hãy tưởng tượng rằng giờ đây chúng ta đang sống trong thời đại mà RSA đã bị phá vỡ, có thể là sau khi sáng chế ra máy tính lượng tử mạnh. Vì vậy, hệ thống của Bennett và Brassard phải độc lập và không phụ thuộc vào RSA. Trong hàng tháng trời, Bennett và Brassard đã cố xoay xở tìm kiếm một cách phân phối chìa khóa mã. Sau đó, vào năm 1984, một lần cả hai đang đứng trên sân ga Croton-Harmon, ở gần Phòng thí nghiệm Thomas J. Watson của hãng IBM. Họ đợi tàu đưa Brassard trở lại Montreal, và giết thời gian bằng cách tán gẫu về những gian nan và phiền phức của Alice, Bob và Eve. Vì tàu đến sớm vài phút, lẽ ra họ đã vẫy chào tạm biệt mà không có thêm bất cứ tiến triển nào về vấn đề phân phối chìa khóa mã. Nhưng thay vì, trong một khoảnh khắc xuất thần, họ đã tạo ra mật mã lượng tử, một loại mật mã an toàn nhất đã từng được phát minh.

Phương pháp mật mã lượng tử của họ đòi hỏi ba bước chuẩn bị trước. Mặc dù các bước này không liên quan đến việc gửi một bức thư mã hóa, song chúng cho phép trao đổi một chìa khóa an toàn để sau đó có thể sử dụng để mã hóa một bức thư.

Bước 1. Alice bắt đầu bằng việc truyền đi một chuỗi ngẫu nhiên các số **1** và **0** (bit), bằng cách lựa chọn một cách ngẫu nhiên các sơ đồ phân cực thẳng (nằm ngang và thẳng đứng) và chéo. Hình 76 cho thấy một chuỗi các phôtôn như vậy đang trên đường đi đến chỗ Bob.

Bước 2. Bob phải đo phân cực của các phôtôn này. Vì anh không biết Alice đã sử dụng sơ đồ phân cực nào cho mỗi phôtôn nên anh hoán đổi ngẫu nhiên máy dò + và máy dò × của mình. Đôi khi Bob chọn đúng máy dò và đôi khi anh chọn sai. Nếu

Bob sử dụng sai máy dò, anh có thể sẽ đoán sai phôtôn của Alice. Bảng 27 trình bày tất cả các khả năng có thể xảy ra. Chẳng hạn, ở dòng đầu tiên, Alice sử dụng sơ đồ phân cực thẳng để gửi số **1**, và vì vậy truyền đi phôtôn ↕; sau đó Bob sử dụng đúng máy dò, nên anh nhận được ↕, và ghi lại đúng số **1** là bit đầu tiên trong chuỗi. Trong dòng thứ hai, Alice vẫn làm như vậy, song Bob sử dụng sai máy dò, nên anh ta có thể nhận được ↔ hoặc ↕, nghĩa là anh có thể ghi lại chính xác là số **1** hoặc sai là số **0**.

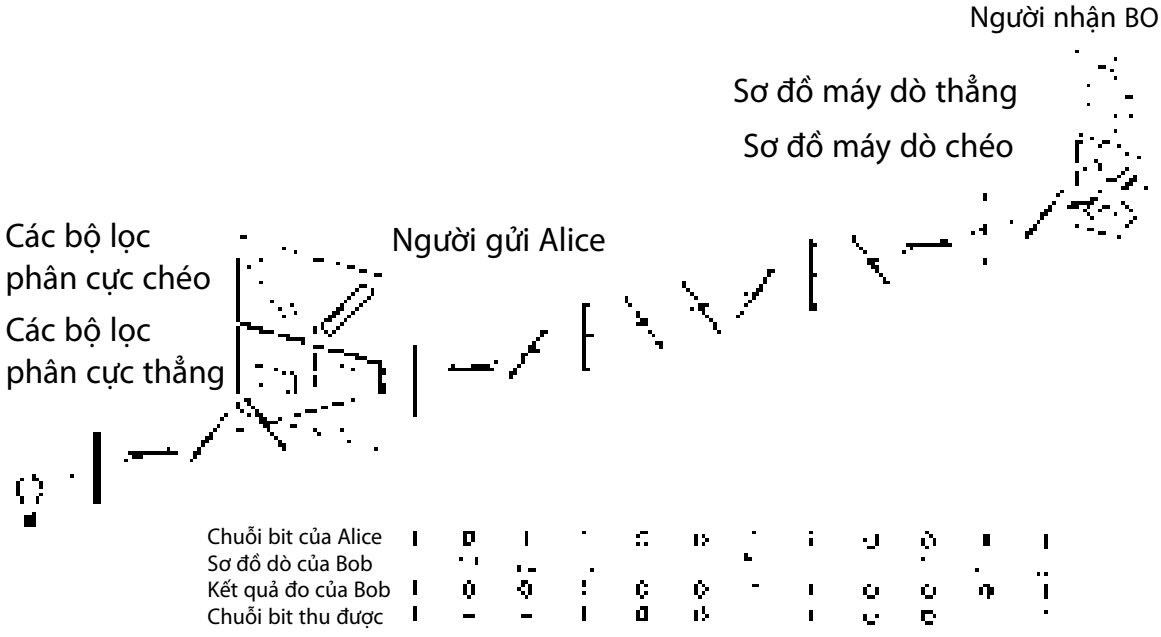
Bước 3. Tới lúc này, Alice đã gửi một chuỗi các số **1** và **0** và Bob đã một vài lần dò đúng và một vài lần sai. Để rà soát lại tình hình, Alice sau đó gọi điện lại cho Bob trên đường dây điện thoại bình thường không an toàn, và nói cho Bob biết sơ đồ phân cực mà cô đã sử dụng cho mỗi phôtôn - song không nói cụ thể phân cực của các phôtôn đó. Như vậy, cô có thể nói rằng phôtôn đầu tiên được gửi đi theo sơ đồ phân cực thẳng, song không nói là cô gửi ↕ hay ↔. Sau đó, Bob nói cho Alice trường hợp nào anh đoán đúng sơ đồ phân cực của cô. Trong những trường hợp đó, anh đo được đúng phân cực và ghi lại đúng số **1** hoặc số **0**. Cuối cùng, Alice và Bob bỏ qua mọi phôtôn mà Bob sử dụng sai sơ đồ, mà chỉ tập trung vào những trường hợp anh đoán đúng. Như vậy, họ đã tạo ra một chuỗi mới các bit ngắn hơn, chỉ bao gồm những đo đạc chính xác của Bob. Toàn bộ bước này được minh họa trong bảng ở cuối Hình 76.

Ba bước trên đã cho phép Alice và Bob thiết lập một chuỗi các số chung, chẳng hạn là **11001001** như ở Hình 76. Tính chất quan trọng của chuỗi này là nó ngẫu nhiên, vì nó xuất phát từ chuỗi ban đầu vốn là ngẫu nhiên của Alice. Hơn nữa, những trường hợp Bob sử dụng đúng máy dò cũng là ngẫu nhiên. Vì

vậy, chuỗi thống nhất của bên gửi và bên nhận không tạo nên một bức thư, nhưng nó có thể sử dụng như là một chìa khóa mã ngẫu nhiên. Rốt cuộc thì quá trình mã hóa an toàn thực sự đã có thể bắt đầu.

Chuỗi được thống nhất ngẫu nhiên này có thể được sử dụng như là chìa khóa mã cho mật mã sổ tay dùng một lần. Chương 3 đã mô tả một chuỗi các chữ cái hoặc chữ số ngẫu nhiên, tức sổ tay dùng một lần, có thể mang lại một mật mã không thể phá vỡ nổi như thế nào - không phải chỉ là hầu như mà là tuyệt đối không thể phá vỡ nổi. Trước đây, vấn đề duy nhất của mật mã sổ tay dùng một lần đó là khó khăn trong việc phân phối một cách an toàn các chuỗi ngẫu nhiên, song sự cải tiến của Bennett và Brassard đã khắc phục được vấn đề này. Alice và Bob đã thống nhất được sổ tay dùng một lần và các quy luật của vật lý lượng tử thực sự đã ngăn không cho Eve chặn bắt được nó. Giờ chính là lúc chúng ta đặt mình vào vị trí của Eve và xem xét tại sao cô ấy lại không thể bắt được chìa khóa mã.

Khi Alice truyền đi các phôtôn phân cực, Eve tìm mọi cách để đo đạc chúng song cô không biết phải sử dụng máy dò + hay máy dò ×. Trong một nửa các trường hợp cô sẽ chọn sai máy dò. Điều này cũng hoàn toàn giống như Bob, vì anh cũng chọn sai máy dò khoảng một nửa số lần. Tuy nhiên, sau khi truyền đi, Alice nói với Bob sơ đồ mà anh cần phải sử dụng đối với mỗi phôtôn và họ thống nhất là chỉ sử dụng các phôtôn được đo khi Bob sử dụng máy dò đúng. Tuy nhiên, điều này không giúp gì được cho Eve vì cô cũng sẽ đo đạc sai một nửa số phôtôn do sử dụng sai máy dò, và vì vậy sẽ dịch sai một vài phôtôn tạo nên chìa khóa mã cuối cùng.



Hình 76 Alice truyền đi một chuỗi các số **1** và **0** cho Bob. Mỗi số **1** và **0** được biểu diễn bằng một phôtôn phân cực, hoặc theo sơ đồ thẳng (nằm ngang/thẳng đứng) hoặc theo sơ đồ chéo. Bob đo phôtôn bằng cách sử dụng máy dò thẳng hoặc chéo của mình. Anh lựa chọn máy dò đúng đối với phôtôn ngoài cùng bên trái và dịch đúng là **1**. Tuy nhiên, anh lại lựa chọn sai máy dò với phôtôn kế tiếp. Anh tình cờ đã dịch đúng là số **0** song bit này sau đó bị loại đi vì anh không chắc chắn là mình đã dò đúng.

Một cách khác để xem xét mật mã lượng tử là dùng một bộ lá bài thay cho các phôtôn phân cực. Mỗi lá bài đều có giá trị và hoa khác nhau, chẳng hạn như quân J cơ hay 6 nhép (chuồn), và thường thì nhìn vào một lá bài chúng ta thấy cả giá trị lẫn hoa cùng lúc. Tuy nhiên, hãy tưởng tượng rằng ta chỉ có thể biết được hoặc là giá trị hoặc là hoa mà không phải là cả hai. Alice rút ra một lá bài và phải quyết định tìm giá trị hay hoa. Giả sử cô lựa chọn tìm hoa, là "bích" và cô ghi lại. Lá bài có thể là 4 bích, song Alice chỉ biết nó là bích. Sau đó, cô chuyển lá bài qua đường dây điện thoại cho Bob. Trong khi điều này diễn ra, Eve tìm cách đoán lá bài, song không may là cô ta lại chọn xác định giá trị, đó là "4". Khi lá bài đến tay Bob, anh quyết định xác định

hoa của nó, vẫn là "bích", và anh ghi lại nó. Sau đó, Alice gọi cho Bob và hỏi xem anh có xác định hoa không, anh đã làm thế và vì vậy Alice và Bob biết rằng họ cùng biết một thứ - đó là cả hai đều ghi lại từ "bích" trong sổ tay của mình. Tuy nhiên, trong khi đó Eve lại ghi trong sổ tay của cô ta là "4", điều này hoàn toàn không có tác dụng gì hết.

Tiếp đó, Alice rút ra một lá bài khác, lần này là con K rô, song một lần nữa, cô chỉ có thể xác định một tính chất mà thôi. Lần

Bảng 27 Các khả năng ở bước hai trong trao đổi phôtôn giữa Alice và Bob

Sơ đồ của Alice	Bit của Alice	Alice gửi	Máy dò của Bob	Máy dò đúng?	Kết quả của Bob	Bit của Bob	Bit của Bob đúng?
Thẳng							
Chéo							

này, cô chọn xác định giá trị, tức là "K" và chuyển lá bài cho Bob qua đường dây điện thoại. Eve cố xác định lá bài và cô cũng chọn xác định giá trị, "K". Khi lá bài đến tay Bob, anh quyết định xác định hoa, tức là "rô". Sau đó, Alice gọi cho Bob và hỏi anh có xác định giá trị của lá bài không và anh thừa nhận là mình đã đoán sai nên lại xác định hoa của nó. Alice và Bob không bận tâm vì họ có thể bỏ qua lá bài này và thử một lá bài khác được chọn ngẫu nhiên từ bộ bài. Trong lần cuối cùng này, Eve đã đúng và xác định giống như Alice, là "K", song lá bài bị loại ra vì Bob đã không xác định đúng. Do vậy Bob không phải lo lắng về sai lầm của mình, vì Alice và anh có thể thống nhất với nhau là bỏ qua nó, song Eve lại sa lầy vào sai lầm của mình. Bằng việc gửi một số lá bài, Alice và Bob có thể thống nhất một chuỗi các giá trị và hoa mà sau đó có thể sử dụng làm cơ sở cho chìa khóa mã.

Mật mã lượng tử cho phép Alice và Bob thống nhất chìa khóa mã, trong khi Eve không thể bắt được chìa khóa mà không có sai sót. Hơn nữa, mật mã lượng tử có thêm một lợi ích nữa: nó cho phép Alice và Bob biết được Eve đang nghe lén. Sự hiện diện của Eve trên đường dây trở nên rõ ràng vì mỗi lần đo đạc một phôtôn, cô đều có nguy cơ là làm biến đổi nó và những biến đổi này đều dễ dàng nhận ra đối với Alice và Bob.

Hãy tưởng tượng rằng Alice gửi đi ↖, và Eve đo đạc nó bằng một máy dò sai, máy dò +. Kết quả là, máy dò + buộc phôtôn ↖ đi ra thành phôtôn ↑ hoặc →, vì đó là cách duy nhất để phôtôn có thể đi qua máy dò của Eve. Nếu Bob đo phôtôn đến này bằng máy dò × thì anh có thể dò được ↗, chính là phôtôn mà Alice đã gửi, hoặc có thể dò được ↖, tức phép đo là sai. Đây là một vấn đề đối với Alice và Bob vì Alice gửi phôtôn phân

cực chéo và Bob đã sử dụng máy dò đúng nhưng anh lại đo nó sai. Tóm lại, khi Eve lựa chọn sai máy dò, cô sẽ "làm xoắn" một số phôtôn và điều này khiến Bob ngả theo hướng sai, ngay cả khi anh sử dụng đúng máy dò. Các sai sót này có thể bị phát hiện nếu Alice và Bob thực hiện quá trình rà soát lỗi không tốn mấy thời gian.

Việc rà soát lỗi được hoàn thành sau ba bước sơ bộ, lúc mà Alice và Bob có các chuỗi số **1** và **0** y hệt nhau. Giả sử là họ đã thiết lập một chuỗi gồm 1.075 chữ số nhị phân. Một cách để Alice và Bob kiểm tra sự tương thích của các chuỗi tương ứng của mình đó là Alice gọi cho Bob và đọc lên toàn bộ chuỗi của mình cho anh. Không may là Eve đang nghe lén và cô ta có thể sẽ bắt được toàn bộ chìa khóa mã. Kiểm tra toàn bộ chuỗi rõ ràng là không khôn ngoan, và cũng không cần thiết. Thay vào đó, Alice chỉ lựa ra 75 chữ số bất kỳ và kiểm tra chúng. Nếu Bob đồng ý với 75 chữ số này thì cũng không chắc là Eve đã nghe lén trong quá trình truyền các phôtôn ban đầu. Trong thực tế, cơ hội mà Eve ở trên đường dây và không ảnh hưởng đến đo đạc của Bob đối với 75 chữ số này là thấp hơn 1 phần tỉ. Vì 75 chữ số này được trao đổi công khai giữa Alice và Bob, nên chúng sẽ bị loại bỏ và sổ tay dùng một lần của họ giảm xuống chỉ còn 1000 chữ số nhị phân. Nói cách khác, nếu Alice và Bob tìm ra một sự không thống nhất trong số 75 chữ số thì họ sẽ biết Eve đã nghe lén, và họ sẽ hủy bỏ toàn bộ sổ tay dùng một lần đó, chuyển sang một đường dây mới và bắt đầu lại từ đầu.

Tóm tắt lại, mật mã lượng tử là một hệ thống bảo đảm độ an toàn cho một bức thư bằng cách làm cho Eve rất khó khăn để đọc được chính xác thông tin giữa Alice và Bob. Hơn nữa, nếu

Eve cố nghe lén thì Alice và Bob có thể phát hiện ra sự hiện diện của cô ta. Vì vậy mật mã lượng tử cho phép Alice và Bob trao đổi và thống nhất sổ tay dùng một lần một cách hoàn toàn bí mật và sau đó họ có thể sử dụng nó như là một chìa khóa để mã hóa thư. Quá trình này gồm năm bước cơ bản:

(1) Alice gửi Bob một chuỗi phôtôn và Bob đo đạc chúng.

(2) Alice nói cho Bob những trường hợp nào Bob đo đúng (mặc dù Alice nói với Bob khi nào Bob đo đúng song cô không nói với anh kết quả đúng là gì, nên cuộc nói chuyện có thể bị ghi âm lại mà không có bất kỳ tổn hại nào đến sự an toàn).

(3) Alice và Bob loại bỏ những đo đạc mà Bob thực hiện sai và tập trung vào những đo đạc đúng để tạo ra một cặp sổ tay dùng một lần giống hệt nhau.

(4) Alice và Bob kiểm tra tính chính xác của sổ tay dùng một lần bằng cách thử một vài chữ số.

(5) Nếu quá trình rà soát thỏa mãn, họ có thể sử dụng sổ tay dùng một lần đó để mã hóa thư; nếu sự rà soát phát hiện ra sai sót, họ biết rằng các phôtôn đã bị Eve ghi lại và họ cần phải bắt đầu lại từ đầu.

Mười bốn năm sau bài báo của Wiesner về tiền lượng tử bị các tạp chí khoa học từ chối, nó đã khởi nguồn cho một hệ thống liên lạc tuyệt đối an toàn. Hiện đang sống ở Israel, Wiesner đã yên lòng rằng thành quả của ông đang được ghi nhận: "Nhìn lại, tôi tự hỏi tại sao tôi không thể làm gì hơn. Người ta phê phán tôi là kẻ trốn chạy vì đã không nỗ lực hơn để ý tưởng của mình được công bố - tôi cho rằng theo nghĩa nào đó họ đúng - song

tôi lúc đó mới chỉ là một nghiên cứu sinh trẻ tuổi và chưa tự tin lắm. Bất luận thế nào, lúc đó dường như không ai có hứng thú với tiền lượng tử".

Các nhà mật mã đã nhiệt thành chào đón mật mã lượng tử của Bennett và Brassard. Tuy nhiên, nhiều nhà thực nghiệm cho rằng hệ thống này vận hành tốt về lý thuyết song sẽ thất bại trong thực tiễn. Họ tin rằng khó khăn trong việc xử lý đối với từng phôtôn riêng lẻ sẽ khiến hệ thống không thể thực hiện được. Mặc cho sự chỉ trích này, Bennett và Brassard vẫn tin chắc rằng mật mã lượng tử có thể vận hành được. Trong thực tế, họ tin tưởng vào hệ thống của mình nhiều đến mức không để ý đến việc chế tạo nó. Như Bennett đã từng nói: "Không có lý do gì phải đến Bắc Cực khi bạn biết chắc rằng nó ở đó".

Tuy nhiên, thái độ hoài nghi ngày càng tăng cuối cùng đã khiến Bennett phải chứng minh rằng hệ thống của mình có thể thực sự vận hành. Năm 1988, ông bắt đầu tích lũy những cấu phần cần thiết cho một hệ thống mã hóa lượng tử, và nhận một nghiên cứu sinh, John Smolin, để giúp lắp ráp thiết bị. Sau một năm nỗ lực, họ đã sẵn sàng thử gửi đi bức thư đầu tiên được mã hóa bởi mật mã lượng tử. Một tối muộn, họ lui vào phòng thí nghiệm cách ly ánh sáng, một môi trường tối để tránh các phôtôn lang thang có thể ảnh hưởng đến thí nghiệm của họ. Sau khi ăn một bữa tối thịnh soạn, họ đã sẵn sàng cho một đêm dài lắp đặt thiết bị. Họ tiến hành gửi các phôtôn phân cực qua căn phòng và sau đó đo đạc chúng bằng một máy dò + và máy dò ×. Một máy tính gọi là Alice thực hiện việc truyền phôtôn và một máy tính gọi là Bob quyết định máy dò nào được sử dụng để đo phôtôn.

Sau nhiều giờ vật lộn, vào khoảng 3 giờ sáng, Bennett đã chứng kiến sự trao đổi mật mã lượng tử đầu tiên. Alice và Bob thực hiện việc gửi và nhận phôtôn, họ trao đổi về các sơ đồ phân cực mà Alice đã sử dụng, họ loại bỏ các phôtôn mà Bob đã đo bằng máy dò sai và thống nhất một sổ tay dùng một lần chứa các phôtôn còn lại. "Không còn nghi ngờ gì nữa, nó đã hoạt động", Bennett nhớ lại, "chỉ có điều là các ngón tay của chúng tôi còn vụng về chế tạo nó mà thôi". Thí nghiệm của Bennett đã chứng minh rằng hai máy tính, Alice và Bob, có thể liên lạc với nhau tuyệt đối an toàn. Đây là một thí nghiệm lịch sử, cho dù một thực tế là hai máy tính chỉ cách nhau có 30 cm."

Từ thí nghiệm của Bennett, thách thức là phải chế tạo được một hệ thống mã hóa lượng tử vận hành trên những khoảng cách hữu ích. Đây không phải là một nhiệm vụ đơn giản vì các phôtôn không đi được xa lắm. Nếu Alice truyền đi một phôtôn với phân cực nhất định qua không khí, các phân tử khí sẽ tương tác với nó, làm thay đổi phân cực mà điều đó thì không thể chấp nhận được. Một môi trường hiệu quả hơn cho việc truyền phôtôn đó là qua dây cáp quang, và các nhà nghiên cứu mới đây đã thành công trong việc sử dụng kỹ thuật này để chế tạo hệ thống mã hóa lượng tử có thể vận hành trên một khoảng cách đáng kể. Năm 1995, các nhà nghiên cứu của Đại học Geneva đã thành công trong việc thực hiện mã hóa lượng tử qua đường dây cáp quang dài 23 km từ Geneva đến một thị trấn ở Nyon.

Gần đây nữa, một nhóm các nhà khoa học ở Phòng Thí nghiệm quốc gia Los Alamos ở New Mexico một lần nữa đã bắt đầu thí nghiệm với mã hóa lượng tử qua không khí. Mục đích cơ bản của họ là muốn tạo nên một hệ thống mã hóa

lượng tử có thể vận hành qua vệ tinh. Nếu điều này có thể đạt được thì chúng ta sẽ có được thông tin liên lạc toàn cầu tuyệt đối an toàn. Đến nay, nhóm Los Alamos đã thành công trong việc truyền đi một chìa khóa mã lượng tử qua không khí với khoảng cách là 1km.

Các chuyên gia an ninh giờ đây đang băn khăn không biết sẽ phải mất bao lâu để mật mã lượng tử trở thành một công nghệ thực tiễn. Hiện tại, việc có mã hóa lượng tử chưa mang lại lợi thế thực sự nào, vì mật mã RSA đã cho phép chúng ta có thể mã hóa không phá vỡ nổi rồi. Tuy nhiên, nếu máy tính lượng tử trở thành hiện thực thì RSA và tất cả các mật mã hiện đại khác sẽ trở nên vô dụng và mã hóa lượng tử sẽ trở nên cần thiết. Vậy là cuộc chạy đua vẫn còn tiếp tục. Vấn đề thực sự quan trọng đó là liệu mã hóa lượng tử có đến kịp thời để cứu chúng ta thoát khỏi mối đe dọa của máy tính lượng tử hay không, hay sẽ có một khoảng thời gian ngăn cách giữa việc tạo ra máy tính lượng tử và sự xuất hiện của mã hóa lượng tử. Đến lúc này thì mã hóa lượng tử đang là công nghệ tiến bộ hơn. Thí nghiệm của người Thụy Sĩ với đường dây cáp quang chứng minh rằng có thể thiết lập một hệ thống cho phép liên lạc an toàn giữa các thiết chế tài chính trong phạm vi một thành phố. Thực tế, hiện đã có thể thiết lập một liên kết mã hóa lượng tử giữa Nhà Trắng và Lầu Năm góc. Mà cũng có thể thực sự đã có một liên kết như vậy ở đó rồi cũng nên.

Mật mã lượng tử có thể sẽ đánh dấu sự kết thúc của cuộc chiến triền miên giữa các nhà tạo mã và giải mã, và các nhà tạo mã sẽ là những người chiến thắng. Mã hóa lượng tử là một hệ thống mã hóa không thể phá vỡ nổi. Điều này có vẻ như là một

sự khẳng định hơi khoa trương, nhất là theo kinh nghiệm của những tuyên bố trước đây. Vào những thời điểm khác nhau trong hơn hai ngàn năm qua, các nhà mật mã đã tin rằng mật mã dùng một bảng chữ cái, mật mã dùng nhiều bảng chữ cái, và mật mã máy như Enigma đều không thể phá vỡ nổi. Trong mỗi trường hợp đó, các nhà tạo mã cuối cùng đều đã bị chứng minh là sai, vì tuyên bố của họ chỉ dựa vào thực tế là sự phức tạp của mật mã của họ bỏ xa sự khéo léo và công nghệ của các nhà giải mã ở một thời điểm trong lịch sử. Với nhận thức muộn màng, chúng ta có thể thấy rằng các nhà giải mã cuối cùng cũng đều tìm ra một cách phá vỡ từng mật mã hoặc khám phá ra một công nghệ có thể phá vỡ mật mã đó cho họ.

Tuy nhiên, tuyên bố rằng mật mã lượng tử là an toàn là tương đối khác biệt so với những tuyên bố trước đây. Mật mã lượng tử không chỉ gần như không thể phá vỡ mà là tuyệt đối không thể phá vỡ nổi. Lý thuyết lượng tử, lý thuyết thành công nhất trong lịch sử vật lý, hàm ý là không thể có khả năng để Eve bắt được chính xác sổ mã dùng một lần được thiết lập giữa Alice và Bob. Eve thậm chí không thể tìm cách chặn bắt sổ mã dùng một lần mà không bị Alice và Bob nghi ngờ bị cô nghe lén. Thực sự thì nếu một bức thư được bảo vệ bởi mật mã lượng tử mà bị giải mã thì điều đó có nghĩa là thuyết lượng tử có sơ hở, và điều này sẽ có những hệ quả tàn phá ghê gớm đối với các nhà vật lý; họ sẽ buộc phải xem xét lại những hiểu biết của họ về sự vận hành của vũ trụ ở cấp độ cơ bản nhất.

Nếu hệ thống mật mã lượng tử có thể được chế tạo để vận hành trên một khoảng cách lớn thì sự tiến hóa của mật mã sẽ dừng lại. Cuộc tìm kiếm sự an toàn cho những bí mật riêng tư

sẽ đi đến hồi kết. Công nghệ sẽ sẵn sàng để bảo đảm thông tin liên lạc an toàn cho các chính phủ, quân đội, hãng kinh doanh và công chúng. Vấn đề duy nhất còn lại là liệu chính phủ có cho phép chúng ta sử dụng nó hay không. Làm thế nào để các chính phủ điều hòa được mật mã lượng tử sao cho nó vừa làm giàu cho Thời đại Thông tin mà không bảo vệ bọn tội phạm?

Một thách thức giải mã:
mười bước tiến đến 15 ngàn đôla

Thách thức Giải mã được khởi xướng từ tháng Chín năm 1999 và vẫn còn chưa giải được kể từ lúc ấn hành. Đây là một cơ hội để bạn thử nghiệm kỹ năng giải mã của mình và để giành lấy giải thưởng trị giá 15.000 đôla. Thách thức này bao gồm mười bước riêng biệt. Bước một là một dạng mật mã dùng một bảng chữ cái khá đơn giản và sau đó các bước còn lại sẽ tiến dần theo lịch sử của khoa học mật mã. Nói cách khác, bước hai gồm một văn bản đã được mã hóa bằng một loại mật mã sớm nhất và bước mười là một dạng mật mã hiện đại nhất. Nhìn chung mỗi bước sẽ khó khăn hơn bước trước nó.

Bạn cần làm gì để giành được giải thưởng?

Giải mã mỗi trong số mười văn bản mật mã bạn sẽ nhận được một bức thư. Ngoài nội dung chính của bức thư, sẽ còn cho biết một từ mã. Để giành giải thưởng, bạn phải có đủ mười từ mã này. Vì vậy phải giải mã tất cả mười bước. Mặc dù bạn có thể

thực hiện các bước theo trình tự nào cũng được, song tôi khuyến nghị nên giải theo đúng trình tự đưa ra. Trong một số trường hợp, giải mã một bước sẽ cung cấp thông tin quan trọng cho việc giải mã bước tiếp theo.

Làm thế nào để được xét giải?

Để được xét giải, xin vui lòng gửi trước hai chữ cái đầu của mỗi từ mã, cùng với tên, địa chỉ và số điện thoại của bạn. Nếu các chữ cái của bạn là đúng, bạn sẽ được thông báo xác nhận trong vòng 28 ngày và yêu cầu gửi mười bản giải mã hoàn chỉnh. Nếu bạn là người đầu tiên xác định đúng mười từ mã, bạn sẽ giành được 15.000 đôla. Tất cả thư từ xin gửi về địa chỉ sau:

The Cipher Challenge, P.O Box 23064,

London W11 3GX, UK.

Người chiến thắng sẽ là người gửi đến đầu tiên theo dấu bưu điện. Không có yếu tố may rủi, chỉ có kỹ năng thành thạo. Xin nhớ, tôi chỉ liên lạc với các thí sinh đã gửi đúng hai chữ cái đầu của mỗi từ mã (đăng ký thành công). Hơn nữa, tôi cũng không thể trả lời mọi thắc mắc liên quan đến Thách thức Giải mã. Mọi cập nhật về thách thức này sẽ được tải lên trang web **Thách thức Giải mã**

http:/www.4thestate.co.uk/cipherchallenge.

Giải thưởng 1 năm

Nếu cho đến ngày 1 tháng Mười năm 2000 không ai giành được giải thưởng, thì 1.500 đôla sẽ được trao cho bất kỳ ai đạt được

nhiều tiến bộ nhất và sớm nhất, tức là hoàn thành được nhiều bước liên tiếp nhất. Nói cách khác, nếu bạn giải được bước 1, 2, 3, 4 và 8 thì chỉ có các bước từ 1 đến 4 là có giá trị tranh giải. Trước khi đăng ký tranh giải thưởng này, bạn nên kiểm tra trang web **Thách thức Giải mã**, trên đó sẽ đưa ra người hiện đang dẫn đầu và mức độ thành công của họ. Nếu bạn tin rằng mình thành công ở bước tiếp theo thì hãy gửi hai chữ cái đầu thuộc từ mã của tất cả những bước mà bạn đã giải mã được cùng với tên, địa chỉ và số điện thoại của bạn. Nếu các chữ cái là đúng, chúng tôi sẽ liên lạc trong vòng 28 ngày để xác nhận các chữ cái đó và yêu cầu bạn gửi toàn bộ các từ mã. Nếu các từ mã của bạn đúng, thì bạn sẽ trở thành người dẫn đầu và thành công của bạn sẽ được đưa lên trang Web. Bất kỳ ai là người dẫn đầu vào ngày 1 tháng Mười năm 2000 sẽ giành được 1.500 đôla. Giải thưởng này hoàn toàn độc lập với giải thưởng 15.000 đôla giành cho người chiến thắng toàn bộ.

Xin gửi thư đến địa chỉ chúng tôi đã đưa ở trên. Một lần nữa, xin nhớ là tôi chỉ liên lạc với những người đã gửi đến hai chữ cái đúng của mỗi từ mã.

Tôi khuyến nghị nên theo dõi sát thông tin trên trang Web, trong đó cũng có các thông tin khác liên quan đến cuốn sách và Thách thức này.

Các quy tắc tranh giải chính thức đối với người đăng ký ở Mỹ và Canada

1. Cuộc thi này được mở ra dành cho mọi công dân cư trú tại Mỹ và Canada (trừ tỉnh Quebec). Đối với quy tắc dự thi cho

"giải thưởng 1 năm", sẽ theo chỉ dẫn của ông Singh. Ngoài giải thưởng 1 năm, Simon Singh sẽ lựa chọn người đầu tiên hoàn thành **Thách thức Giải mã** thành công tính đến ngày 1 tháng Một năm 2010. Nếu không ai khám phá được hết tất cả 10 từ mã đến ngày 1 tháng Một năm 2010, thì lời giải sẽ được công bố trên trang Web, và Singh, theo suy xét của ông, sẽ quyết định ai là người có nhiều tiến triển nhất, tức là người hoàn thành được nhiều bước liên tiếp nhất. Nếu người chiến thắng là công dân của Mỹ hoặc Canada, thì người chiến thắng sẽ được trao 15.000 đôla.

2. Những người đăng ký phải gửi đến cho Singh trước ngày 1 tháng Một năm 2010.

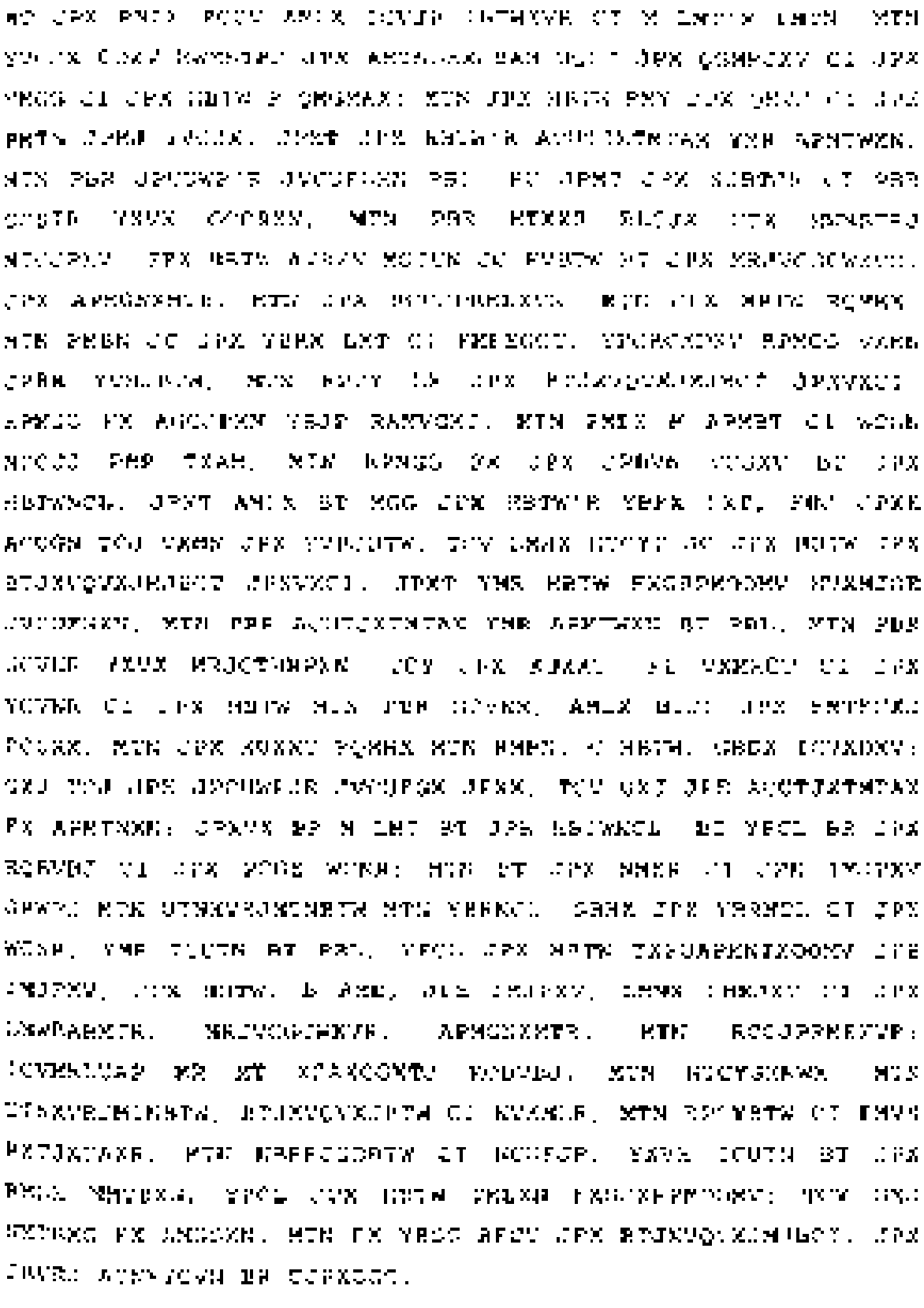
3. Người chiến thắng sẽ được Singh lựa chọn từ những người đã được nhận. Quyết định của ông Singh sẽ là quyết định cuối cùng. Người chiến thắng sẽ được thông báo xác nhận chiến thắng trong vòng 28 ngày, hoặc trong trường hợp là người chiến thắng hoàn thành nhiều bước liên tiếp nhất đến ngày 1 tháng Một năm 2010 sẽ được thông báo vào ngày 1 tháng Hai năm 2010. Người chiến thắng sẽ có 30 ngày kể từ ngày thông báo để chấp nhận giải thưởng nếu không người khác sẽ được chọn. Ông Singh không chịu trách nhiệm đối với những người chậm trễ, thất lạc hoặc không trực tiếp đăng ký.

4. Người chiến thắng có thể được yêu cầu thực hiện một bản tuyên thệ đủ tư cách và chấp nhận tự do quảng cáo (Promotional Release). Tham gia cuộc thi bao gồm việc cho phép được sử dụng tên, chân dung, dữ liệu tiểu sử và đăng ký tham gia cho các mục đích công khai và quảng cáo mà không được nhận thêm tiền thù lao.

5. Các nhân viên của Random House Inc., các chi nhánh và văn phòng đại diện của nó và thành viên gia đình của họ không được phép tham dự cuộc thi này. Cuộc thi dành cho mọi công dân cư trú của Mỹ và Canada trên 18 tuổi tính đến ngày đăng ký. Trừ những nơi nào có sự ngăn cấm hoặc hạn chế bởi luật pháp. Áp dụng cho tất cả các bang, liên bang và các định chế địa phương. Thuế, nếu có, là trách nhiệm của người đoạt giải.

6. Để biết tên người được giải, sẽ có sau ngày 1 tháng Tư năm 2010 và cho đến 1 tháng Mười năm 2010, hãy gửi một phong bì có dán tem và địa chỉ bản thân đến The Cipher Challenge, P.O Box 23064, London W11 3GX, UK.

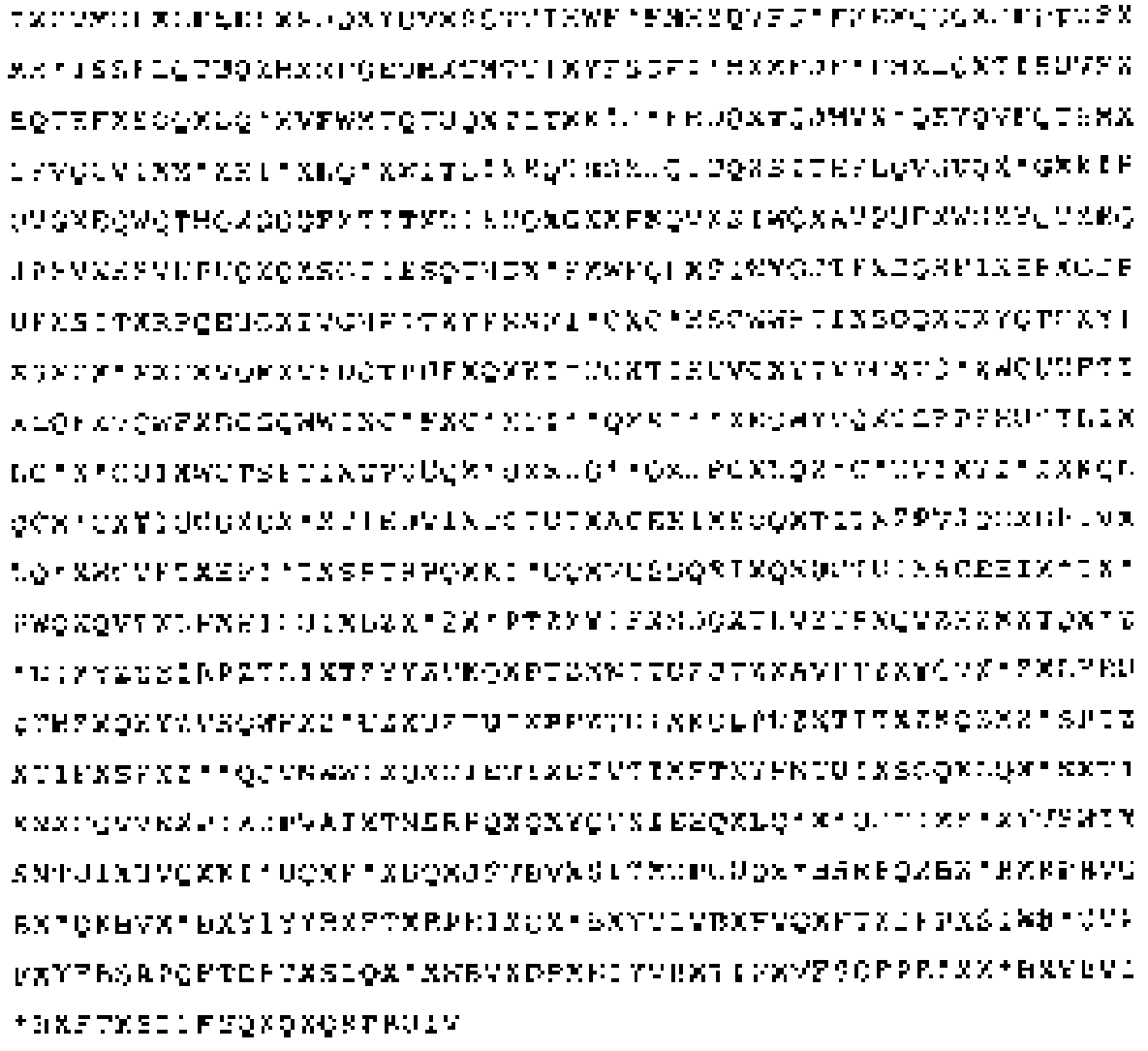
Bước 1: Mật mã thay thế đơn giản dùng một bảng chữ cái



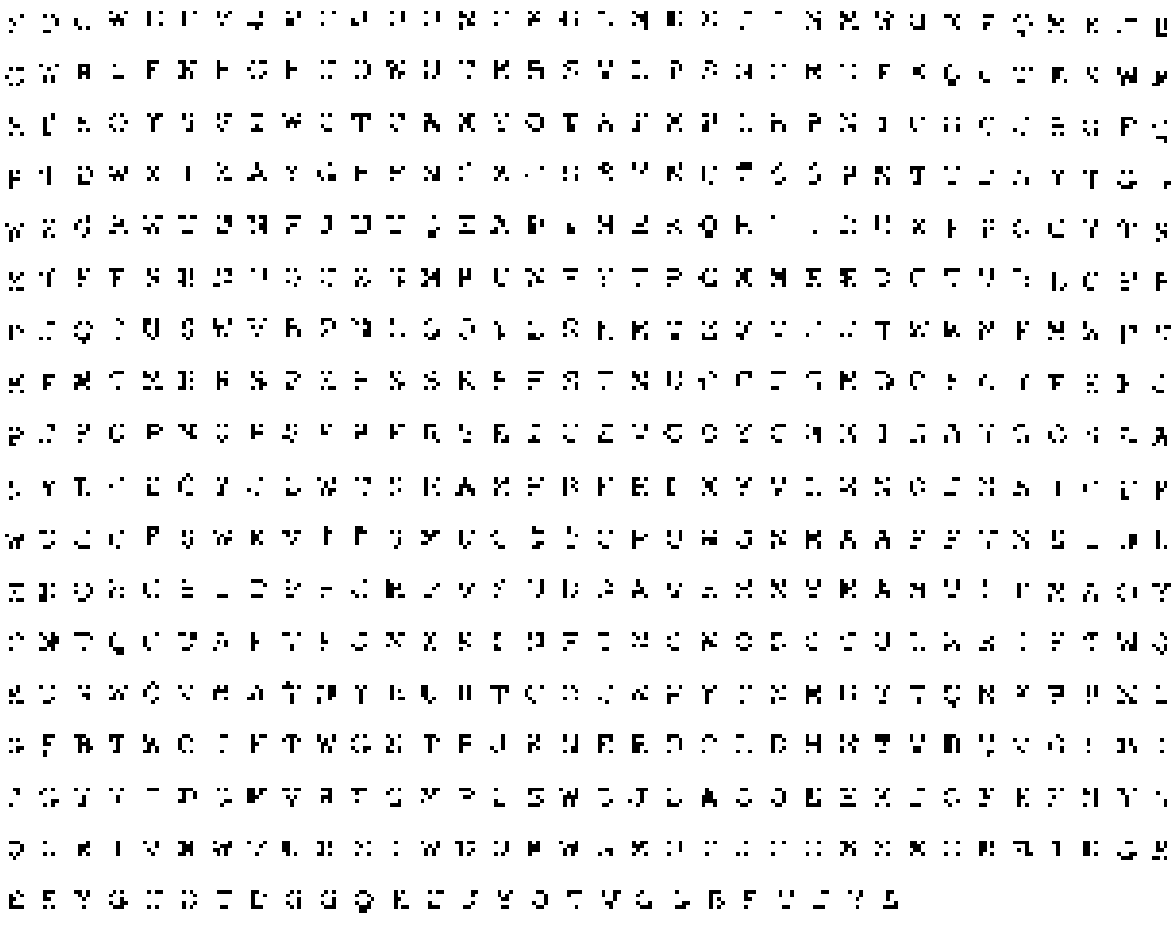
Bước 2: Mật mã dịch chuyển Caesar

MHILY LZA ZBHL XBPZXBL MVYABUHL HWWPBZ JSHBKPBZ JHLJBZ
XPJABT HYJHUBT LZA ULBAYVU

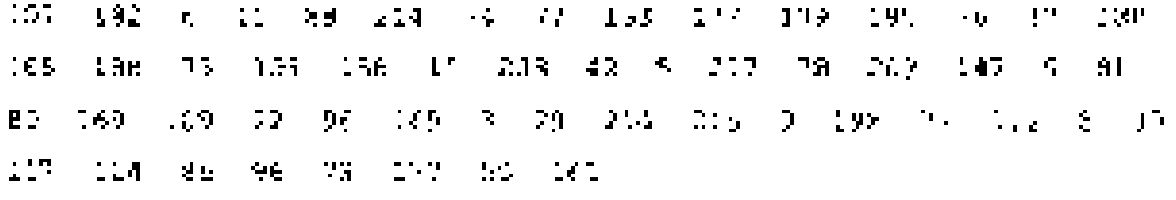
Bước 3: Mật mã dùng một bảng chữ cái kết hợp với các từ đồng âm



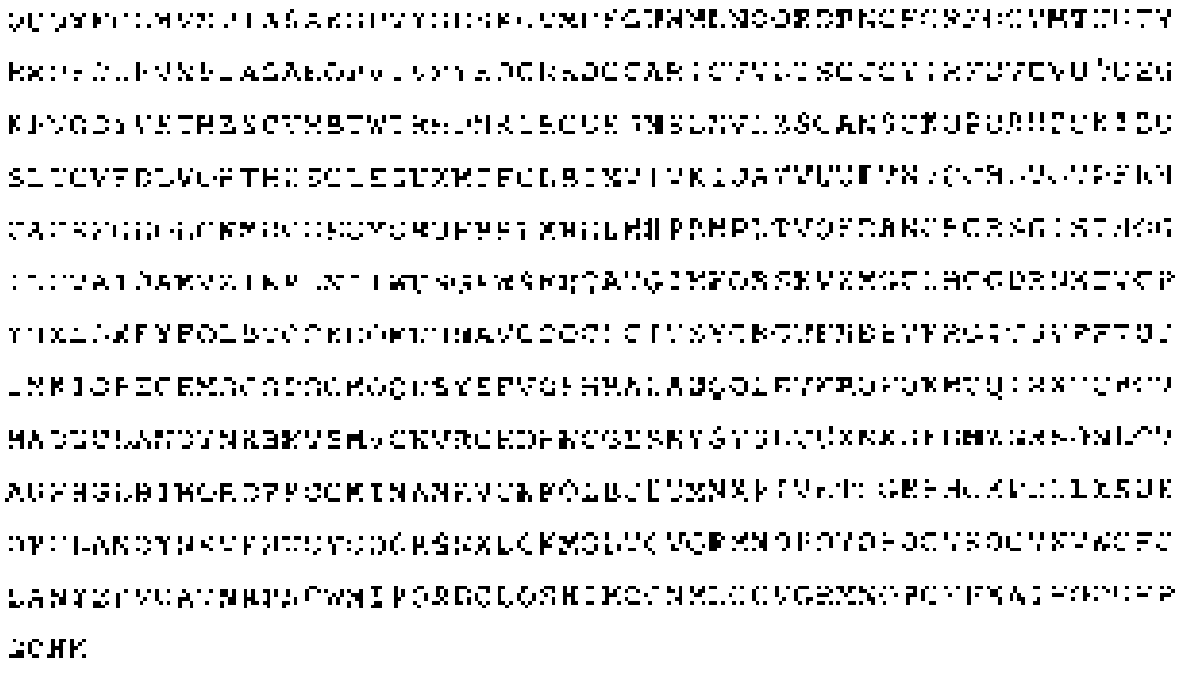
Bước 4: Mật mã Vigenère



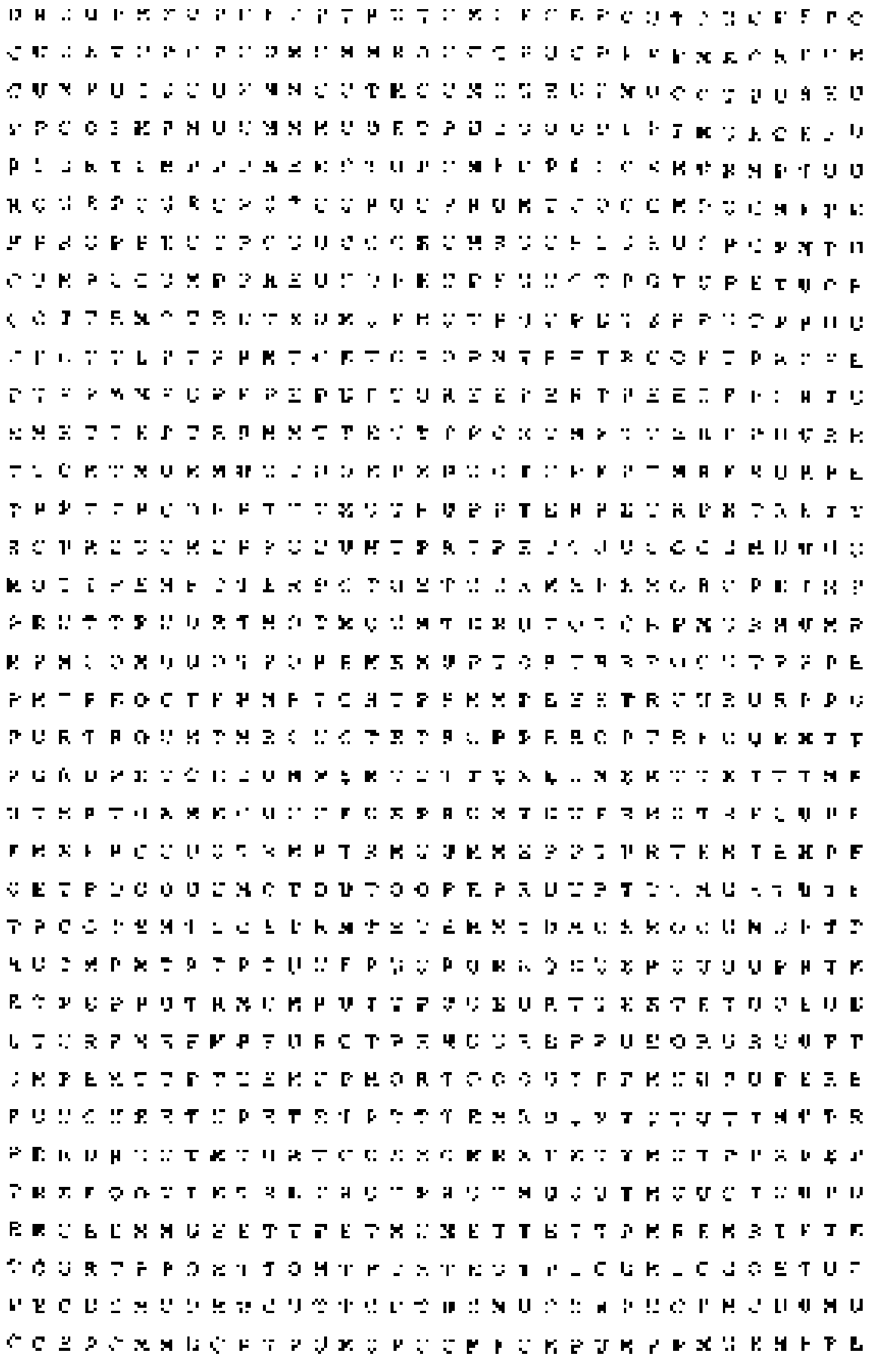
Bước 5

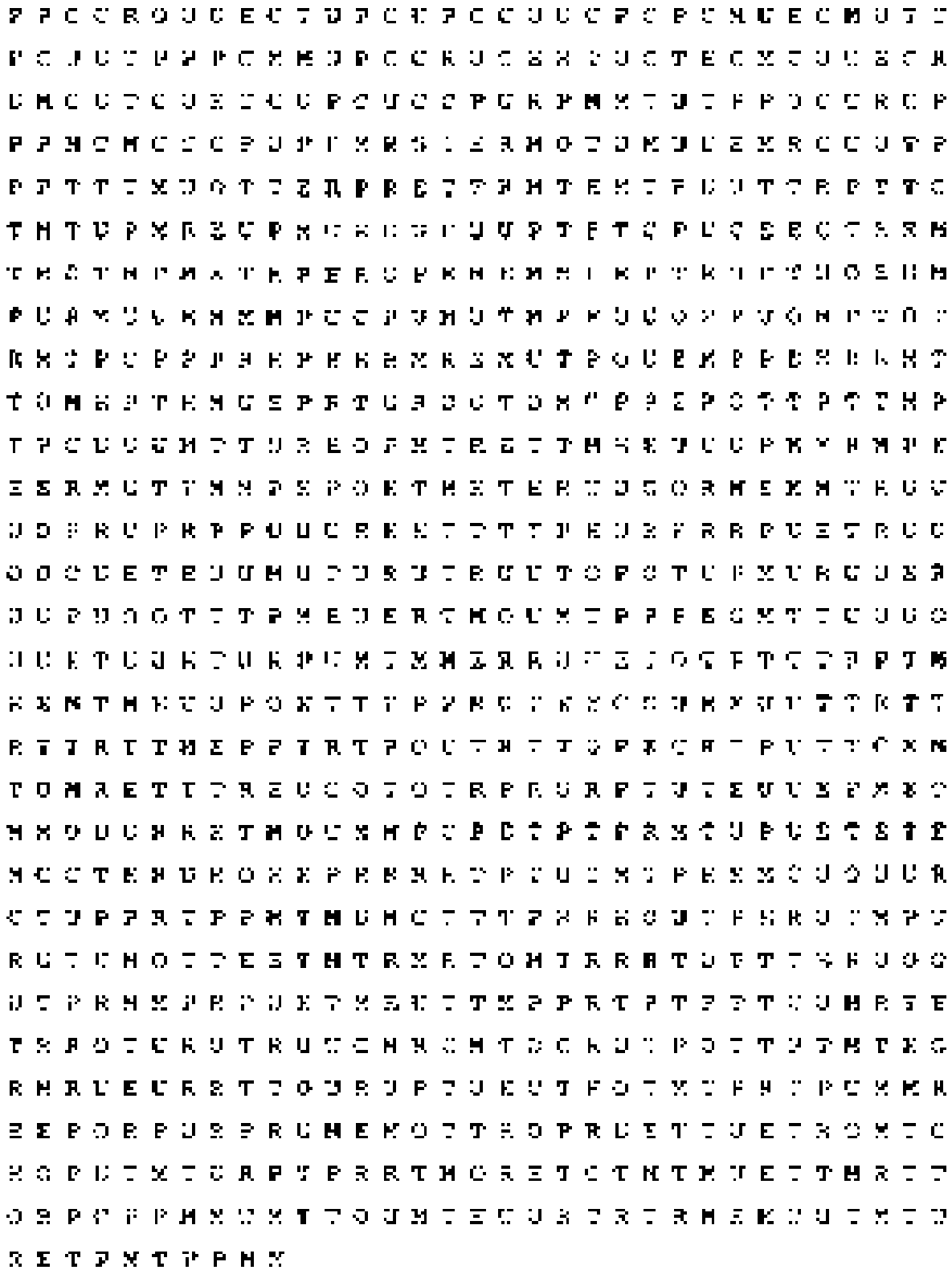


Bước 6

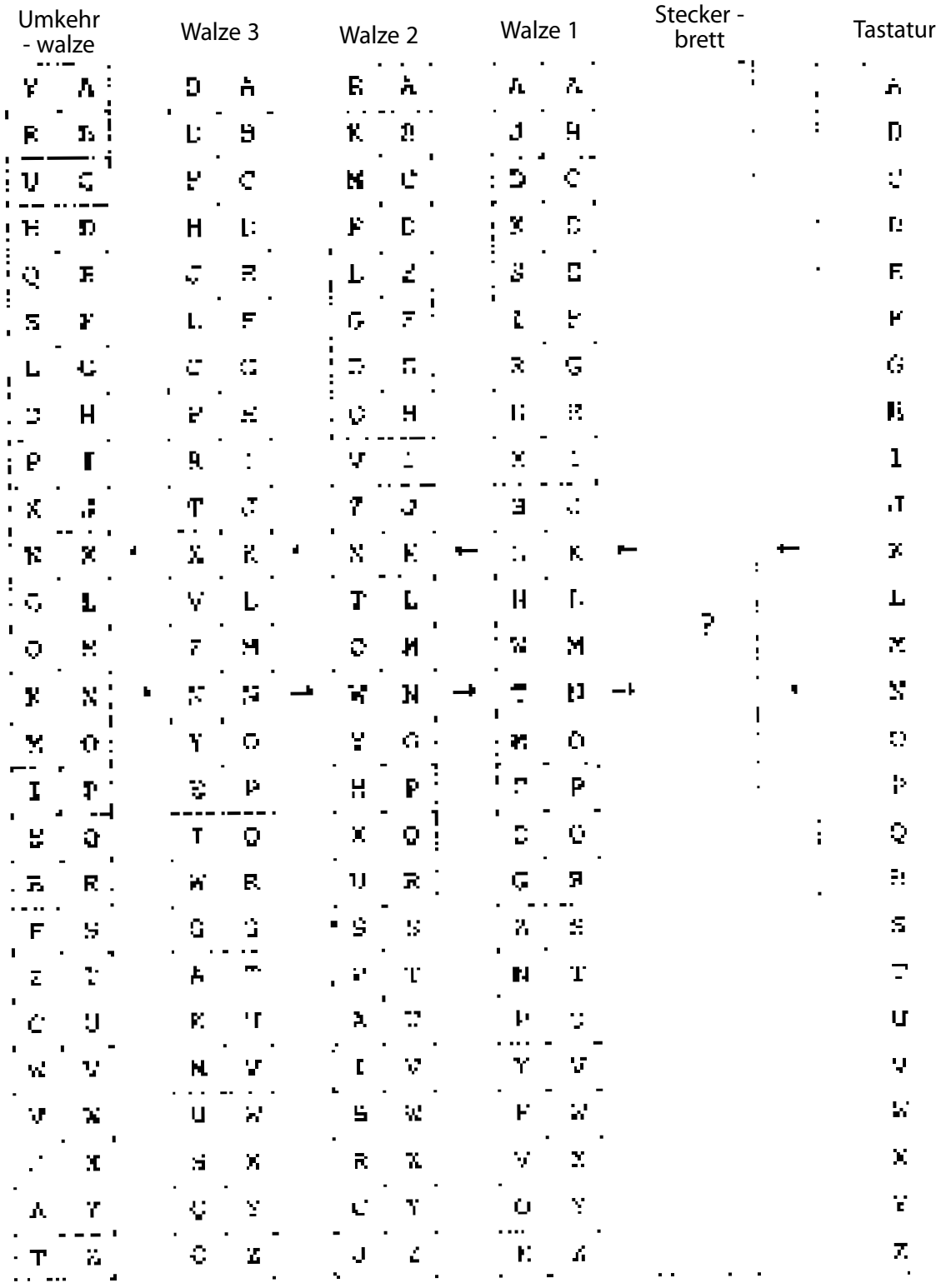


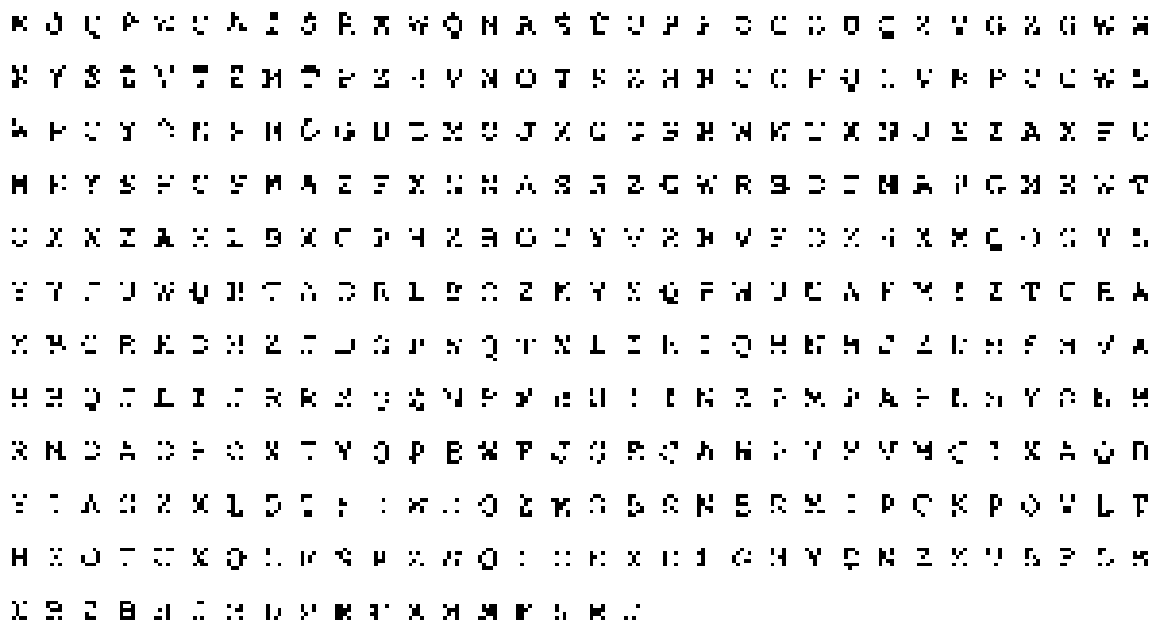
Bước 7





Bước 8





Bước 9

```
begin 600 cover.uu
[illegible]
end
```

Bước 10:

thư ngắn:

```
10652 30975 22294 17534 12990 86421 15456 85924 58239 26672 10125
11442 99199 09294 87259 20201 56839 80952 42340 99110 70a2d 91754
21685 25575 4e849 "4E50 85629 33365 23356 30C94 55674
```

thư dài:

```
\rogie: 500 text.d
M.&■i>S 1;3.'.4;%A•\%T•V/(AW!:H4GB55;T;'U KMA^.JB:X■D|.:XF A>X
MXI9QO:37\IONGSAL•$A?A'BP32Y3X•■t^.'2%'37?2 6O'l.7 O/ 'T OG-*
MNHZA:Q■3X|3^U:L^E2%ZAJ%S^F■9F?^:/0&<)1.:KSAJ' W1:(\:BSRGFNO
M.MEaB^C0%:KUDICW5VU:FG.DTJ?2+■Y  7:\ ■>3O*>JW•O.ZT.•BUW55.7%
4:GAU9+I■;'P•I>i'4<•Z•:.7.W\
```

```
4CX1
```

Phụ lục A

Đoạn mở đầu cuốn A Void của Georges Perec do Gilbert Adair dịch

Today, by radio, and also on giant hoardings, a rabbi, an admiral notorious for his links to masonry, a trio cardinals, a trio, too, of insignificant politicians (bought and pay for by a rich and corrupt Anglo-Canadian banking corporation), inform us all of how our country now risks dying of starvation. A rumor, that's my initial thought as I switch off my radio, a rumor or possibly a hoax. Propaganda, I murmur anxiously - as though, just by saying so, I might allay my doubts - typical politiian's propaganda. But public opinion gradually absorbs it as a fact. Individuals start strutting around with stout clubs. "Food, glorious food!" is a common cry (occasionally sung to Bart's music), with ordinary hardworking folk harassing officials, both local and national, cursing capitalists and captains. Cops shrink from going out on night shift. In Mâcon a mob storms a municipal building. In Rocadamour ruffians rob a hangar full of foodstuff, pillaging tons of tuna fish, milk and cocoa, as also a vast quantity of corn-all of it, alas, totally unfit for human comsumption. Without fuss or ado, and naturally without any sort of trial, an indignant crowd hangs 26 solicitors on hastily

built scaffold in front of Nancy's law courts (this Nancy is a town, not a woman) and ransacks a local journal, a disgusting right-wing rag that is siding against it. Up and down this land of ours looting has brought docks, shop and farms to virtual standstill.

Lần đầu tiên xuất bản tại Pháp với cái tên *La Disparition* ở NXB Editions Denoel năm 1969 và tại Anh bởi Harvill năm 1994.

(Chú ý rằng toàn bộ đoạn văn trên trong tác phẩm gốc của Perec và bản dịch của Adair đều không có một chữ cái **e** nào - ND).

Phụ lục B

Một vài mẹo cơ bản trong phân tích tần suất

(1) Bắt đầu bằng việc đếm tần suất của tất cả các chữ cái trong bản mật mã. Có khoảng năm chữ cái có tần suất ít hơn 1%, và các chữ cái này có thể biểu diễn các chữ **j**, **k**, **b**, **x** và **z**. Một trong các chữ cái có thể có tần suất lớn hơn 10% và nó có thể biểu diễn chữ **e**. Nếu bản mật mã không tuân theo sự phân bố tần suất như vậy thì nên xét đến khả năng là bức thư gốc không được viết bằng tiếng Anh. Bạn có thể xác định ngôn ngữ bằng việc phân tích phân bố tần suất trong bản mật mã. Ví dụ, đặc trưng trong tiếng Ý là có ba chữ cái có tần suất lớn hơn 10%, và chín chữ cái có tần suất nhỏ hơn 1%. Trong tiếng Đức, chữ cái **e** có tần suất đặc biệt cao là 19%, vậy nên bất kỳ bản mật mã nào có chứa một chữ cái với tần suất cao như vậy thì chắc chắn đó là tiếng Đức. Một khi bạn đã xác định được ngôn ngữ, bạn nên sử dụng một bảng tần suất thích hợp cho ngôn ngữ mà bạn phân tích. Thường thì vẫn có thể giải bức mật mã ở dạng ngôn ngữ không quen thuộc nếu bạn có một bảng tần suất thích hợp.

(2) Nếu sự tương quan với tiếng Anh được khẳng định, song văn bản thường vẫn chưa lộ ra ngay lập tức, mà sẽ thường là như vậy, thì hãy tập trung vào các cặp chữ cái lặp lại. Trong

tiếng Anh, các chữ cái lặp lại thường xuyên nhất là **ss**, **ee**, **tt**, **ff**, **ll**, **mm** và **oo**. Nếu văn bản mật mã có chứa các ký tự lặp lại nào như vậy, bạn có thể giả định chúng biểu thị cho một trong các cặp trên.

(3) Nếu văn bản mật mã có chứa khoảng cách giữa các từ thì cố gắng xác định các từ chỉ có một, hai hoặc ba chữ cái. Các từ chỉ có một chữ cái trong tiếng Anh là **a** và **I**. Các từ có hai chữ cái thường gặp là **of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am**. Từ có ba chữ cái thường gặp nhất là **the** và **and**.

(4) Nếu có thể, hãy dựng một bảng tần suất đối với bức thư mà bạn đang thử giải mã. Ví dụ, các bức thư trong quân sự thường có xu hướng bỏ qua các đại từ và mạo từ, và các từ bị mất thường là **I, he, a** và **the** sẽ làm giảm tần suất của một số chữ cái thường gặp nhất. Nếu bạn biết mình đang tấn công một bức thư quân sự thì bạn nên sử dụng một bảng tần suất tạo từ các bức thư quân sự khác.

(5) Một trong các kỹ năng hữu dụng nhất cho một nhà phân tích mật mã đó là khả năng xác định các từ, hay thậm chí toàn bộ cụm từ, dựa trên kinh nghiệm hoặc hoàn toàn phỏng đoán. Al Khalil, một nhà phân tích mật mã ả rập đầu tiên đã chứng tỏ tài năng này khi ông hóa giải được một bản mật mã của người Hy Lạp. Ông đã đoán rằng bản mật mã bắt đầu bằng lời chào "Nhân danh Thượng đế". Sau khi đặt các chữ cái này tương ứng với một đoạn trong văn bản mật mã, ông đã sử dụng chúng làm đòn bẩy để mở ra phần còn lại của bản mật mã. Như đã biết, đó được gọi là một crib.

(6) Trong một số trường hợp, chữ cái thường gặp nhất trong văn bản mật mã có thể là **E**, chữ cái thường gặp tiếp theo là **T**,

và v.v... Nói cách khác, tần suất của các chữ cái trong văn bản mật mã ăn khớp với các tần suất trong bảng tần suất. Chữ **E** trong văn bản mật mã hóa ra lại chính là chữ **e** thực, và điều tương tự cũng đúng với các chữ cái khác, song văn bản mật mã trông thật lộn xộn. Trong trường hợp này, bạn không phải đang gặp phải một mật mã thay thế mà là một mật mã chuyển vị. Tất cả các chữ cái biểu thị cho chính nó, song chúng được đặt sai vị trí.

Cuốn Phân tích mật mã của Helen Fouché Gaines (Dover) là một bản hướng dẫn tốt. Cùng với việc cung cấp các mẹo, nó còn có các bảng tần suất chữ cái của một số ngôn ngữ, và cung cấp một danh sách các từ thường gặp nhất trong tiếng Anh.

Phụ lục C

Mật mã Kinh thánh

Năm 1997, cuốn Mật mã Kinh thánh của Michael Drosnin đã được phổ biến sâu rộng trên khắp thế giới. Drosnin đã tuyên bố rằng Kinh thánh có chứa những thông điệp ẩn giấu có thể được khám phá bằng cách tìm chuỗi những chữ cái cách đều nhau (EDLS). EDLS được tìm ra bằng cách lấy một đoạn bất kỳ, chọn ra chữ cái đầu tiên, sau đó nhảy cách mỗi lần một số nhất định các chữ cái. Ví dụ, với đoạn... Michael Drosnin caused headlines around the world..., chúng ta bắt đầu bằng chữ "M" trong từ Michael và nhảy cách, ví dụ 5 chữ cái mỗi lần. Nếu ta ghi lại những chữ cái thứ 5, chúng ta sẽ có EDLS là **mesahirt**...

Mặc dù EDLS trong trường hợp này không chứa từ nào có nghĩa, song Drosnin đã mô tả sự khám phá ra một số lượng đáng kinh ngạc các EDLS trong Kinh thánh không chỉ tạo nên các từ có nghĩa mà còn hình thành các câu hoàn chỉnh. Theo Drosnin, các câu này chính là những lời tiên tri của kinh thánh. Chẳng hạn, ông tuyên bố đã tìm thấy sự ám chỉ đến các vụ ám sát John F. Kenedy, Robert Kennedy và Anwar Sadat. Trong một EDLS, tên của Newton được nhắc đến bên cạnh lực hấp dẫn và trong một EDLS khác, cái tên Edison gắn với bóng đèn.

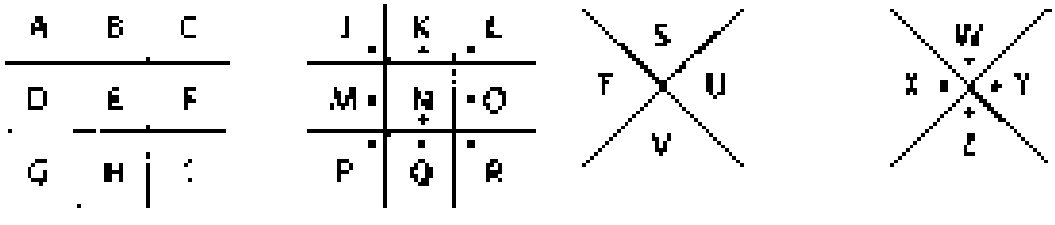
Mặc dù cuốn sách của Drosnin dựa trên một bài báo đã công bố của Doron Witzum, Eliyahu Rips và Yoav Rosenberg, song những tuyên bố của nó còn tham vọng hơn nhiều và đã thu hút được rất nhiều lời phê bình. Nguyên nhân chính của mối quan tâm này là văn bản được nghiên cứu rất dài: với một đoạn văn bản đủ dài thì không có gì đáng ngạc nhiên nếu tạo ra được các cụm từ có ý nghĩa bằng cách thay đổi vị trí bắt đầu và độ dài bước nhảy.

Brendan McKay của Đại học Quốc gia Australia đã thử chỉ ra điểm yếu trong phương pháp của Drosnin bằng việc tìm các EDLS trong cuốn Moby Dick, và khám phá được 13 mệnh đề có nói đến các vụ ám sát những người nổi tiếng, trong đó có Trotsky, Gandhi và Robert Kenedy. Hơn nữa, các văn tự tiếng Hebrew được thừa nhận là có nhiều EDLS một cách đặc biệt, vì chúng hầu như không có nguyên âm. Điều đó có nghĩa là người dịch có thể chèn thêm vào các nguyên âm khi nào họ thấy thích hợp, điều đó khiến cho rất dễ dàng rút ra các tiên đoán.

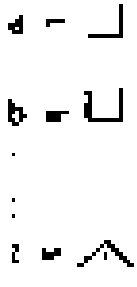
Phụ lục D

Mật mã chuồng heo

Mật mã thay thế dùng một bảng chữ cái vẫn tiếp tục tồn tại qua nhiều thế kỷ dưới nhiều hình thái khác nhau. Chẳng hạn, mật mã chuồng heo được các thành viên của Hội Tam điểm sử dụng trong những năm 1700 để giữ bí mật các sổ sách ghi chép của mình và ngày nay vẫn được các em học sinh sử dụng. Mật mã này không phải là thay thế một chữ cái này bằng một chữ cái khác mà là thay thế mỗi chữ cái bằng một ký hiệu theo bốn hình mẫu dưới đây.



Để mã hóa một chữ cái cụ thể, hãy tìm vị trí của nó ở một trong bốn hình ở trên, sau đó vẽ góc tương ứng có chứa chữ cái đó. Chẳng hạn:



Nếu bạn đã biết chìa khóa mã, thì mật mã chuồng heo rất dễ giải. Còn nếu không, thì nó cũng rất dễ dàng bị phá vỡ bởi:

(Đoạn mã này có nghĩa là: Frequency Analysis - Phân tích tần suất - ND)

Phụ lục E

Mật mã Playfair

Mật mã Playfair được phổ biến bởi Lyon Playfair, vị nam tước Playfair đầu tiên của St. Andrews, song lại do Ngài Charles Wheatstone, một trong những nhà tiên phong của điện tín, phát minh. Hai người sống gần nhau ở hai bên cây cầu Hammersmith, và họ thường gặp nhau để trao đổi những ý tưởng về mật mã.

Mật mã này thay thế mỗi cặp chữ cái liền nhau trong văn bản thường bằng một cặp chữ cái khác. Để mã hóa và chuyển một bức thư, người gửi và người nhận trước tiên phải thống nhất với nhau một từ chìa khóa. Chẳng hạn, chúng ta có thể sử dụng chính tên của Wheatstone là Charles làm từ chìa khóa. Sau đó, trước khi mã hóa, các chữ cái trong bảng chữ cái được ghi vào các ô của một hình vuông 5×5, trong đó hai chữ cái I và J ghi trong cùng một ô (chú ý rằng sau khi ghi lần lượt các chữ cái trong từ chìa khóa - ở đây là Charles - vào các ô, các chữ cái còn lại được ghi vào bảng theo đúng thứ tự của bảng chữ cái - ND):

C	H	A	R	L
E	S	B	D	F
G	I/J	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

Tiếp đó, bức thư thường được phân thành các cặp chữ cái hay chữ ghép. Hai chữ cái trong bất kỳ chữ ghép nào phải khác nhau, điều này đạt được, như trong ví dụ dưới đây, bằng cách chèn thêm chữ **x** vào giữa hai chữ **m** trong từ **hammersmith**, và thêm chữ **x** vào vị trí cuối cùng để tạo nên một chữ ghép cho chữ cái cuối cùng còn lẻ ra:

Văn bản thường (gặp tôi ở cầu Hammersmith tối nay)
mett me at hammersmith bridge tonight
Văn bản thường sau khi đã ghép đôi các chữ cái:
me-et-me-at-ha-mx-me-rs-mi-th-br-id-ge-to-ni-tx

Việc mã hóa giờ đã có thể bắt đầu. Tất cả các chữ ghép rơi vào một trong ba nhóm: cả hai chữ cái ở cùng một hàng, hoặc cùng một cột, hoặc không cùng hàng, cùng cột. Nếu cả hai chữ cái ở cùng một hàng, thì chúng được thay bằng chữ cái nằm ngay bên phải mỗi chữ; như vậy thì **mi** trở thành **NK**. Nếu một trong hai chữ cái nằm ở cuối hàng thì sẽ được thay bằng chữ cái ở đầu hàng đó; như vậy **ni** trở thành **GK**. Nếu cả hai chữ cái ở cùng một cột, chúng được thay bằng chữ cái ở ngay dưới nó; như vậy **ge** trở thành **OG**. Nếu một trong các chữ cái ở cuối cột thì sẽ được thay thế bằng chữ cái ở đầu cột đó; như vậy **ve** trở thành **CG**.

Nếu các chữ cái của chữ ghép không cùng hàng cũng không cùng cột thì người mã hóa tuân theo một quy tắc khác. Chữ

cái đầu tiên được thay thế bằng chữ cái nằm ở giao của hàng chứa chữ cái thứ nhất với cột chứa chữ cái thứ hai; còn chữ cái thứ hai trong cặp được thay thế bởi chữ cái nằm ở giao của hàng chứa chữ cái thứ hai với cột chứa chữ cái thứ nhất. Như vậy, **me** trở thành **GD**, và **et** trở thành **DO**. Việc mã hóa hoàn tất như sau:

Văn bản thường sau khi đã ghép đôi các chữ cái:
me et me at ha mx me rs mi th br id ge to ni gh tx
Văn bản mật mã:
GD DO GD RQ AR KY GD HD NK PR DA MS OG UP GK IC QY

Người nhận, do cũng biết từ chìa khóa, nên có thể dễ dàng giải bản mật mã trên bằng cách đơn giản là đảo ngược lại quá trình: chẳng hạn, các chữ cái mã hóa trong cùng một hàng sẽ được giải mã bằng cách thay thế chúng bằng các chữ cái đứng bên trái.

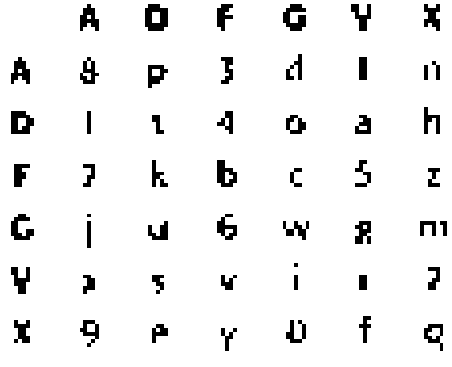
Không những là một nhà khoa học, Playfair còn là một nhân vật có tiếng tăm (Người phát ngôn của Hạ viện, Tổng cục trưởng Tổng cục Bưu điện, và ủy viên về sức khỏe cộng đồng, người đã hỗ trợ cho sự phát triển các cơ sở hiện đại của vệ sinh môi trường). Ông đã quyết định quảng bá ý tưởng của Wheatstone trong số những chính trị gia cao cấp nhất. Ông đề cập đến nó trong một bữa tối vào năm 1854 trước mặt Hoàng tử Albert và Thủ tướng tương lai, Thượng nghị sĩ Palmerston và sau đó ông đã giới thiệu Wheatstone với Thứ trưởng Bộ Ngoại giao. Không may là vị Thứ trưởng này phàn nàn rằng hệ thống quá phức tạp để sử dụng trong điều kiện chiến tranh, đáp lại, Wheatstone tuyên bố rằng ông có thể dạy phương pháp này cho các cậu học sinh của trường tiểu học gần nhất chỉ trong 15 phút. "Rất có thể", vị Thứ trưởng đáp, "song ông không bao giờ có thể dạy điều đó cho các tùy viên".

Mật mã Playfair vẫn dai dẳng tồn tại và cuối cùng Bộ Chiến tranh Anh đã bí mật chấp thuận kỹ thuật này, có lẽ nó đã được sử dụng lần đầu tiên trong cuộc chiến tranh với người Boer (người Phi gốc Đức). Mặc dù đã tỏ ra có hiệu quả trong một thời gian, song mật mã Playfair không phải khó đến mức không phá vỡ nổi. Nó có thể bị phá vỡ bằng cách tìm kiếm các chữ ghép xuất hiện thường xuyên nhất trong bản mật mã và giả định nó biểu thị cho các chữ ghép thường gặp nhất trong tiếng Anh như: **th**, **he**, **an**, **in**, **er**, **re**, **es**.

Phụ lục F

Mật mã ADFGVX

Mật mã ADFGVX mang đặc tính của cả mã thay thế và chuyển vị. Sự mã hóa bắt đầu bằng việc vẽ một bảng kẻ ô vuông 6 × 6 và điền vào 36 ô sự sắp xếp ngẫu nhiên của 26 chữ cái và 10 chữ số. Mỗi hàng và mỗi cột của bảng được nhận dạng bởi một trong 6 chữ cái A, D, F, G, V, X. Sự sắp xếp các thành phần trong các ô đóng vai trò là một phần của chìa khóa mã nên người nhận phải biết trước các chi tiết của bảng để giải mã.



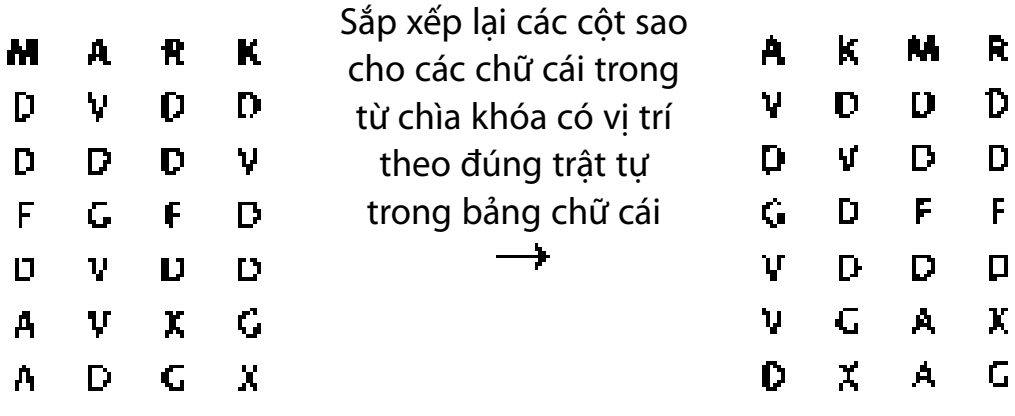
Bước đầu tiên của việc mã hóa là lấy mỗi chữ cái trong bức thư, rồi xác định vị trí của nó trong bảng và thay thế nó bằng các chữ cái đứng đầu hàng và cột của nó. Chẳng hạn, **8** được thay thế bằng **AA**, và **p** sẽ được thay thế bằng **AD**. Dưới đây là một bức thư ngắn được mã hóa theo hệ thống này:

Thư	attack at 10 pm (tấn công vào lúc 10 giờ tối)
Văn bản thường	**a t t a c k a t 1 0 p m**
Bản mật mã bước 1	**DV DD DD DV FG FD DV DD AV XG AD GX**

Lúc này, đây là mật mã thay thế đơn giản dùng một bảng chữ cái và chỉ cần dùng phương pháp phân tích tần suất cũng đủ để phá vỡ nó. Tuy nhiên, bước thứ hai của mật mã ADFGVX là chuyển vị làm cho việc giải mã trở nên khó khăn hơn nhiều. Sự chuyển vị phụ thuộc vào một từ mã, trong ví dụ này là từ **MARK**, và phải cho người nhận biết trước. Sự chuyển vị được thực hiện theo cách thức sau. Trước hết, các chữ cái trong từ chìa khóa được viết trên hàng đầu tiên của một bảng mới. Sau đó, bản mật mã bước 1 được viết bên dưới thành các hàng như được trình bày dưới đây. Các cột trong bảng sau đó được sắp xếp lại để các chữ cái trong từ chìa khóa có vị trí theo đúng trật tự trong bảng chữ cái. Văn bản mã hóa cuối cùng thu được bằng cách ghi lại các chữ cái theo trật tự mới dọc theo các cột từ trên xuống.

Văn bản mật mã cuối cùng là

V D G V V D D V D D G X D D F D A A D D F D X G



Bản mật mã cuối cùng sẽ được truyền đi bằng mã Morse và người nhận sẽ đảo ngược quá trình mã hóa để thiết lập lại văn bản ban đầu. Toàn bộ bản mật mã được tạo bởi chỉ 6 chữ cái (tức là **A**, **D**, **F**, **G**, **V**, **X**), vì các chữ cái này là nhãn của các hàng và cột trong bảng 6×6 ban đầu. Người ta thường tự hỏi tại sao các chữ cái này lại được chọn mà không phải là **A**, **B**, **C**, **D**, **E**, **F**. Câu trả lời là **A**, **D**, **F**, **G**, **V**, **X** nhìn sẽ rất khác nhau khi chuyển sang các chấm và vạch của mã Morse, nên lựa chọn các chữ cái này sẽ giảm thiểu nguy cơ sai sót trong quá trình truyền tín hiệu.

Phụ lục G

Điểm yếu của sự quay vòng sổ tay dùng một lần

Vì nhiều lý do đã được giải thích trong Chương 3, các văn bản mật mã được mã hóa theo sổ tay dùng một lần là không thể giải mã được. Tuy nhiên, điều này là đúng chỉ nếu mỗi sổ tay phải được sử dụng một lần và chỉ một lần. Nếu chúng ta bắt được hai bản mật mã khác nhau được mã hóa bởi cùng một sổ tay dùng một lần, chúng ta có thể giải mã chúng theo cách dưới đây.

Rất có thể là đúng khi ta giả sử rằng bản mật mã đầu tiên có chứa từ **the** ở đâu đó và vì vậy nhà giải mã bắt đầu từ giả định rằng toàn bộ bức thư chứa một chuỗi các từ **the**. Sau đó, chúng ta tìm ra sổ tay dùng một lần cần thiết để biến toàn bộ các từ **the** thành bản mật mã thứ nhất. Đây là dự đoán đầu tiên của chúng ta về sổ tay dùng một lần. Làm thế nào chúng ta biết được phần nào trong sổ tay dùng một lần phỏng đoán này là đúng?

Chúng ta có thể áp dụng dự đoán đầu tiên của mình về sổ tay dùng một lần vào bản mật mã thứ hai, và xem kết quả có ý nghĩa nào không. Nếu may mắn, chúng ta có thể phân biệt được một nhóm các từ trong văn bản thường thứ hai, cho thấy phần tương ứng trong sổ tay dùng một lần là đúng. Đến lượt

mình, điều này sẽ cho chúng ta biết phần nào trong bức thư thứ nhất là từ **the**.

Bằng cách mở rộng các đoạn mà chúng ta tìm thấy trong văn bản thường thứ hai, chúng ta có thể tìm ra thêm về sổ tay dùng một lần và sau đó suy ra các đoạn mới trong văn bản thường thứ nhất. Bằng cách mở rộng các đoạn trong văn bản thường thứ nhất, chúng ta lại tìm ra thêm về sổ tay dùng một lần và sau đó lại suy ra các đoạn mới trong văn bản thường thứ hai. Chúng ta có thể tiếp tục quá trình này cho đến khi giải mã được cả hai.

Quá trình này cũng tương tự như việc giải mã một bức thư được mã hóa bằng mật mã Vigenère sử dụng chìa khóa mã có chứa một chuỗi các từ, chẳng hạn như ví dụ ở chương 3, trong đó chìa khóa mã là **CANADABRAZILEGYPTCUBA**.

Phụ lục H

Giải đáp Ô chữ trên tờ *Daily Telegraph*

Hàng Ngang

1. Troupe
4. Short Cut
9. Privet
10. Aromatic
12. Trend
13. Great deal
15. Owe
16. Feign
17. Newark
22. Impale
24. Guise
27. Ash
28. Centre bit
31. Token
32. Lame dogs
33. Racing
34. Silencer
35. Alight

Hàng Dọc

1. Tipstaff
2. Olive oil
3. Pseudonym
5. Horde
6. Remit
7. Cutter
8. Tackle
11. Agenda
14. Ada
18. Wreath
19. Right nail
20. Tinkling
21. Sennight
23. Pie
25. Scale
26. Enamel
29. Rodin
30. Bogie

Phụ lục I

Một số bài tập dành cho độc giả quan tâm

Một số giải mã vĩ đại nhất trong lịch sử đã được thực hiện bởi những người nghiệp dư. Ví dụ, Georg Grotenfend, người đã thực hiện đột phá đầu tiên trong việc diễn giải các chữ viết hình nêm chỉ là một giáo viên trung học. Đối với các độc giả cảm thấy bức xúc muốn đi theo dấu chân của ông, thì hiện vẫn có một số văn bản chưa giải mã được như Linear A, một văn bản của người Minoa, đã thách thức mọi nỗ lực giải mã, một phần là do tư liệu quá nghèo nàn. Văn bản của người Etrusa thì không gặp khó khăn đó, vì có sẵn 10 000 văn bản để nghiên cứu, nhưng nó đã làm thất bại những học giả vĩ đại nhất. Các văn bản của người Iberi - một loại chữ viết tiền La Mã - cũng chưa thể giải mã được.

Văn tự châu Âu cổ đại hấp dẫn nhất xuất hiện trên Đĩa Phaitos độc nhất vô nhị được phát hiện ở phía Nam Crete vào năm 1908. Đó là một tấm hình tròn có niên đại khoảng 1700 trước CN mang một văn bản có dạng hai đường xoắn ốc, mỗi đường ở một bên. Các ký hiệu này không có cảm tưởng làm bằng tay, mà là làm bằng nhiều con dấu, làm cho văn bản này là ví dụ cổ xưa nhất về đánh máy. Điều đáng nói là không có một văn bản tương tự nào khác đã được tìm thấy, vì vậy việc giải mã chỉ dựa trên một

lượng thông tin rất hạn chế, chỉ có 242 ký tự được phân thành 61 nhóm. Tuy nhiên, văn bản đánh máy này cho thấy nó được sản xuất hàng loạt, nên có thể hy vọng rằng các nhà khảo cổ sẽ phát hiện ra cả kho những đĩa tương tự, ngõ hầu có thể làm sáng tỏ thứ chữ viết còn bí ẩn này.

Một trong những thách thức lớn nhất ở ngoài châu Âu là giải mã thứ chữ viết vào Thời đại Đồ đồng của nền văn minh Indus mà người ta tìm thấy trên hàng ngàn dấu gắn xi có niên đại ở thiên niên kỷ thứ ba trước CN. Mỗi dấu gắn xi có vẽ một con vật kèm theo một câu viết ngắn, nhưng ý nghĩa của chúng còn là một thách đố đối với các chuyên gia. Một ví dụ đặc biệt là văn tự được tìm thấy trên một tấm gỗ lớn với các chữ cái cao tới 37cm. Đó có thể là một bảng cáo thị cổ nhất thế giới. Từ đây có thể suy ra rằng không chỉ giới quý tộc mới biết chữ và đặt ra câu hỏi điều gì được thông báo ở đây. Câu trả lời khả dĩ nhất, đây là chiến dịch ca tụng công đức của nhà vua và nếu danh tính của nhà vua có thể xác lập được thì bản cáo thị này có thể sẽ cung cấp cho ta cách tiếp cận phần còn lại của văn bản này.

Phụ lục J

Toán học của mật mã RSA

Những điều trình bày dưới đây là sự mô tả toán học dễ hiểu về cơ chế mã hóa và giải mã RSA.

(1) Alice lấy hai số nguyên tố cực lớn, p và q, nhưng để đơn giản ta lấy $p = 17$ và q = 11. Hai con số này Alice phải giữ bí mật hoàn toàn.

(2) Alice nhân hai số này với nhau và nhận được số N. Trong trường hợp đang xét $N = 187$. Bây giờ cô lấy một số e khác. Trong trường hợp này cô chọn $e = 7$. (Thực ra, e và $(p - 1)\times(q - 1)$ phải nguyên tố cùng nhau, tức không có ước số chung khác 1. Nhưng đây chỉ là một chi tiết mang tính kỹ thuật).

(3) Bây giờ Alice có thể công bố công khai số N và số e trên báo hoặc trong danh bạ điện thoại, chẳng hạn. Vì hai số này cần có để mã hóa nên nó phải có sẵn cho bất kỳ ai muốn mã hóa các thư gửi cho Alice. Hai con số này được gọi chung là chìa khóa mã công khai. (Ngoài việc là một bộ phận của chìa khóa mã công khai của Alice, số e cũng có thể là một bộ phận trong chìa khóa mã công khai của bất kỳ ai khác. Tuy nhiên, mỗi người lại phải có một số N khác nhau, tùy thuộc vào việc chọn các số p và q của họ).

(4) Để mã hóa một bức thư, trước hết phải biến bức thư đó thành một con số *M*. Ví dụ, một từ được biến đổi thành các chữ số nhị phân theo ASCII và các số nhị phân này có thể được xem như một số thập phân *M*. Sau đó M được mã hóa để cho văn bản mật mã (*C*) theo công thức
$C = Me \pmod N$

(5) Hãy tưởng tượng Bob chỉ muốn đơn giản gửi cho Alice một cái hôn: chỉ là chữ cái X. Trong ASCII nó được biểu diễn bởi số nhị phân 1011000, số này tương đương với số 88 trong hệ thập phân.
Vậy $M = 88$.

(6) Để mã hóa bức thư này, Bob bắt đầu bằng cách tìm chìa khóa mã công khai của Alice và phát hiện ra rằng $N = 187$ và $e = 7$. Những con số này cùng với công thức mã hóa cho phép Bob dễ dàng mã hóa bức thư. Với $M = 88$, thay vào công thức mã hóa ta được:
$C = 88^7 \pmod{187}$

(7) Tính *C* theo công thức này bằng máy tính bỏ túi là điều không dễ dàng, vì màn hình không hiển thị nổi một số lớn như vậy. Tuy nhiên, có một mẹo khá hiệu quả để tính các hàm lũy thừa với số mũ lớn trong số học đồng dư.

Chúng ta biết rằng $7 = 4 + 2 + 1$,

$887 \pmod{187} = [884 \pmod{187} \times 882 \pmod{187} \times 881 \pmod{187}] \pmod{187}$

$881 = 88 = 88 \pmod{187}$

$882 = 7744 = 77 \pmod{187}$

$884 = 59\,969\,536 = 132 \pmod{187}$

$$887 = 881 \times 882 \times 884 = 88 \times 77 \times 132 = 894\,432 = 11 (\text{mod } 187)$$

Bây giờ Bob gửi văn bản mã hóa $C = 11$ cho Alice.

(8) Chúng ta biết rằng các hàm số mũ trong số học đồng dư là các hàm một chiều, do vậy sẽ là rất khó tính ngược lại để phục hồi bức thư gốc *M*. Do đó Eve không thể giải mã được bức thư đó.

(9) Tuy nhiên, Alice dễ dàng giải mã được bức thư, vì cô đã có trong tay một thông tin đặc biệt, đó là giá trị của các số nguyên tố *p* và *q*. Cô tính được một số đặc biệt, đó là số *d*, được biết là chìa khóa riêng của cô. Số *d* được tính theo công thức sau:

$e \times d = 1 (\text{mod}(p-1) \times (q-1))$,

$7 \times d = 1 (\text{mod } 16 \times 10)$

$7 \times d = 1 (\text{mod } 160)$

Suy ra $d = 23$.

(Việc suy ra giá trị của *d* không phải là quá dễ dàng, nhưng một kỹ thuật được gọi là thuật toán Euclid sẽ cho phép Alice tìm được giá trị của *d* một cách tương đối nhanh chóng và dễ dàng).

(10) Để giải mã bức thư, Alice đơn giản chỉ cần dùng công thức sau $M = Cd \ (\text{mod } N)$

$M = 11^{23} \ (\text{mod } 187)$

$M = [111(\text{mod } 187) \times 112(\text{mod } 187) \times 114(\text{mod } 187) \times 1116(\text{mod } 187)](\text{mod}187)$

$M = 11 \times 121 \times 55 \times 154 \ (\text{mod } 187)$

Suy ra M = 88 = X trong ASCII.

Rivest, Shamir và Adleman đã tạo ra một hàm một chiều đặc biệt mà nó chỉ nghịch đảo được đối với những ai có trong tay thông tin đặc quyền, cụ thể là các giá trị của p và q. Mỗi một hàm có thể được cá thể hóa bằng cách chọn p và q, hai số nhân với nhau cho ta giá trị của N. Hàm này cho phép mọi người mã hóa các bức thư gửi cho một người cụ thể bằng cách chọn số N của người đó, nhưng chỉ người này mới có thể giải mã được các bức thư đó, vì chỉ có người đó mới biết các số p và q, và do đó là người duy nhất biết chìa khóa giải mã là số d.

Các trang WEB tham khảo

- Về bí mật kho báu của Beale:
  http://www.roanokeva.com/stories/beale.html
- Về Bletchley Park:
  http://www.cranfield.ac.uk//bpark/
- Trang chủ về Alan Turing:
  http://www.turing.org.uk/turing/
- Các máy mô phỏng Enigma:
  http://www.attlabs.att.co.uk/andyc/enigma/enigma_j.html
  http://www.izzy.net/-ian/enigma/applet/index.html
- Về Phil Zimmermann và PGP:
  http://www.nai.com/products/security/phil/phil.asp
- Về trung tâm tính toán lượng tử:
  http://www.qubit.org/
- Về nhóm an ninh thông tin, Trường Royal Hollway College:
  http://isg.rhbnc.ac.uk/
- Về bảo tàng quốc gia chuyên về mật mã:
  http://www.nsa.gov:8080/museum/
- Về Hội Mật mã Hoa Kỳ (ACA):
  http://www.und.nodak.edu/org/crypto/crypto/

- Về Tạp chí Mật mã:
  http://www.dean.usma.edu/math/resource/pubs/cryptolo/index.htm
- Các câu hỏi thường xuyên về mật mã:
  http://www.cis.ohio-state.edu/hypertext/faq/usenet/
- Các câu hỏi thường xuyên về mật mã (RSA) ngày nay:
  http://www.rsa.com/rsalabs/faq/html/question.html
- Các liên kết về mật mã:
  http://www.ftech.net/-monark/crypto/web.htm

MẬT MÃ

Simon Singh

Phạm Văn Thiều - Phạm Thu Hằng dịch

Chịu trách nhiệm xuất bản:
Giám đốc - Tổng biên tập NGUYỄN MINH NHỰT
Chịu trách nhiệm nội dung:
Phó giám đốc - Phó tổng biên tập NGUYỄN THẾ TRUẬT
Biên tập: NGUYỄN THỊ HẢI VÂN
Biên tập tái bản:
NGUYỄN PHAN NAM AN - PHẠM TRỌNG LIÊM CHÂU
Bìa: BÙI NAM
Trình bày: ĐỖ VẠN HẠNH

NHÀ XUẤT BẢN TRẺ
161B Lý Chính Thắng - Quận 3 - Thành phố Hồ Chí Minh
ĐT: 39316289 - 39316211 - 38465595 - 38465596 - 39350973
Fax: 84.8.8437450 - E-mail: hopthubandoc@nxbtre.com.vn
Website: http://www.nxbtre.com.vn

CHI NHÁNH NHÀ XUẤT BẢN TRẺ TẠI HÀ NỘI
Số 21, dãy A11, khu Đầm Trấu, p. Bạch Đằng,
q. Hai Bà Trưng, Hà Nội
ĐT: (04)37734544 - Fax: (04)35123395
E-mail: chinhanh@nxbtre.com.vn

CÔNG TY TNHH SÁCH ĐIỆN TỬ TRẺ (YBOOK)
161B Lý Chính Thắng, P.7, Q.3, Tp. HCM
ĐT: 08 35261001 – Fax: 08 38437450
Email: info@ybook.vn
Website: www.ybook.vn

Mật mã
Từ cổ điển đến lượng tử

Chúng ta đang sống trong xã hội thông tin. Đã có truyền tin thì thường có yêu cầu bí mật, và khi đó mật mã trở thành vấn đề trung tâm. Có bí mật quốc gia, có bí mật quân sự, có bí mật công nghệ, có bí mật kinh tế, và rất nhiều bí mật cá nhân nữa.

Có thể nói toàn bộ lịch sử tiến hóa của loài người đều liên quan đến mật mã, đến cuộc đấu tranh liên miên giữa người tạo mật mã và người phá mật mã. Cuốn sách "Mật mã - Từ cổ điển đến lượng tử" vừa đề cập đến bề dày lịch sử của chủ đề này, vừa khai thác những khía cạnh bí hiểm, hấp dẫn của nó.

Trong cách viết, tác giả đã phối hợp tài tình kịch tính của nhiều câu chuyện lý kỳ trong số phận con người, trong các cuộc chiến tranh... với đặc trưng khoa học cũng như sự tinh tế về mặt kỹ thuật phát triển qua nhiều thời đại. Bạn đọc sẽ thỏa mãn về những lời giải thích toán học và kỹ thuật rõ ràng, đồng thời sẽ bị cuốn theo rất nhiều bí mật được tiết lộ.

Hiện nay, Internet được sử dụng hết sức phổ biến. Tuy nhiên, hình như chúng ta chưa quan tâm đầy đủ đến vấn đề bảo mật trên mạng. Do đó, cuốn sách cũng là một lời cảnh tỉnh chung và có tính thời sự rõ ràng. Chuyện mật mã rất bí hiểm, cao xa, nhưng nhiều khi lại rất cụ thể, đơn giản.

"Singh đã quay chúng ta như chong chóng bằng những câu chuyện đầy âm mưu liên quan đến mật mã trong từng chương sách".
—The Wall Street Journal

"Đọc cuốn sách này là cả một niềm vui sướng lớn lao".
—Chicago Tribune

facebook.com/nhaxuatbantre
nxbtre.com.vn